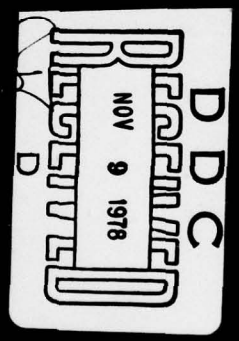
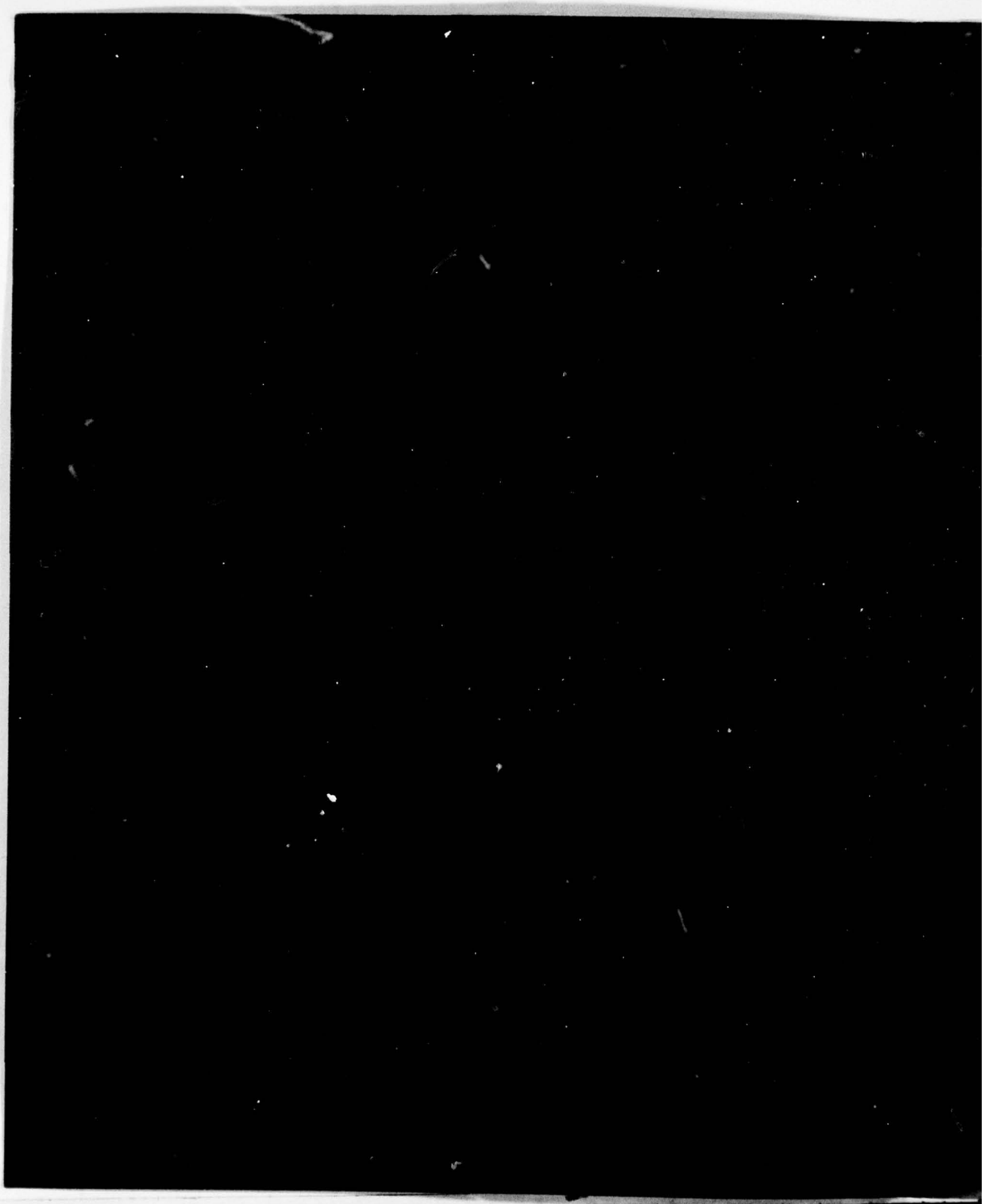
AD-A061 076 HARRY DIAMOND LABS ADELPHI MD F/G 17/4
COMMUNICATION WARFARE.(U)
JUL 78 D J TORRIERI
UNCLASSIFIED HDL-TR-1859 NL

END
DATE FILMED
1-79
DDC





DEPARTMENT OF THE ARMY
HARRY DIAMOND LABORATORIES
2800 POWDER MILL ROAD
ADELPHI, MD. 20783

DELHD-TR

25 October 1978

SUBJECT: Corrections to HDL-TR-1859

TO: Recipients of HDL-TR-1859, Communication Warfare,
by Don J. Torrieri, July 1978

The following should replace paragraphs 5 and 2 on pages 8 and 39, respectively, of the referenced report.

The introduction of cryptographic devices into a communication system causes a performance degradation, an increase in jamming susceptibility, a decrease in reliability, and an increase in cost. Thus, the desirability of cryptographic devices should be carefully considered.

The introduction of cryptographic devices into a communication system causes a performance degradation, an increase in jamming susceptibility, a decrease in reliability, and an increase in cost. Thus, the desirability of cryptographic devices should be carefully considered.

FOR THE COMMANDER:

Ruth E. Savage

RUTH E. SAVAGE
Chief, Technical Reports Branch

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER (14) HDL-TR-1859	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) (6) Communication Warfare		5. TYPE OF REPORT & PERIOD COVERED (9) Technical Report
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(a) (10) Don J. Torrieri		8. CONTRACT OR GRANT NUMBER(a)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Harry Diamond Laboratories 2800 Powder Mill Road Adelphi, MD 20783		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS (16) Program Ele.: 65702A1L765702D671
11. CONTROLLING OFFICE NAME AND ADDRESS U.S. Army Materiel Development and Readiness Command Alexandria, VA 22333		12. REPORT DATE (11) July 1978
		13. NUMBER OF PAGES 54
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) (12) 55 p.		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

DDC RECEIVED NOV 9 1978 D

18. SUPPLEMENTARY NOTES

HDL Project: 1227V1
DRCMS Code: 675702.6710012

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Communication warfare
Electronic countermeaures (ECM)
Electronic countercountermeasures (ECCM)
Pulsed jamming
Jamming
Cryptographic digital communications
Adaptive antenna systems

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The fundamental principles of modern communication warfare are examined. The effectiveness of various types of jamming against amplitude-modulation, phase-modulation, frequency-modulation, and frequency-shift keyed systems is analyzed and assessed. The optimal pulse duration for the pulsed jamming of digital communications is determined. Cryptographic digital communication is reviewed. The potential susceptibility of the

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

1 SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

163050

associated synchronization system to pulsed jamming is considered. Spread-spectrum systems, which conceal the existence of transmissions and resist jamming, are discussed. An example of an adaptive antenna system is analyzed. The main features of optical communication are briefly summarized.

LEVEL II

CONTENTS

FIGURES

EXECUTIVE SUMMARY

Communication warfare is an element of warfare that pits potential communicators against hostile forces which seek to intercept, interpret, and/or disrupt the communications.

In this paper, we discuss various jamming techniques used in communication warfare, compare the efficiencies of certain of these, and indicate alternatives available to the communicators.

Communication Jamming versus Radar Jamming

In order not to waste available power, the potential jammer must first intercept the communications and perhaps locate the receivers. Even if special measures are not employed by the communicators, the interception of communications is generaly more difficult than interception of radar because the communication energy is usually not directed toward the jammer and the transmitted power is low compared with radar. Assuming that the presence of the communications has been established, the jammer faces a situation different from the radar case. Although the communication system uses relatively low power, the jamming signal must compete with a transmitted signal traveling a one-way path, not the two-way path of radar. The jammer is often farther from the communication receiver than the communication transmitter is, while in the radar case the jammer is usually at a distance from the radar system comparable to the length of the return path of the radar signal. Although the jammer can limit the range of a communication system, there is still some range within which communication is possible.

Narrowband and Wideband Jamming

If the communication frequencies can be accurately estimated, narrowband jamming can be employed against the communicators. This type of jamming not only allows economical use of power, but also makes it easy for the jammer to avoid jamming his own communication systems. If frequency-estimation equipment is not used, or if accurate frequency estimation is impossible because of rapid frequency changes or other unfavorable conditions, the jammer can employ wideband jamming. In this case, the jamming energy is spread over large spectral regions to increase the probability that some jamming energy will interfere with the enemy communications.

Response to Jamming

Ordinarily, the jammer cannot ascertain the effectiveness of the jamming. However, effective jamming may force the communication system to change the operating frequency. If the jammer can detect this change

in frequency, he has an important indication that the jamming is indeed disrupting communications. The jammer may then attempt to change the center frequency of the jamming signal accordingly.

In order to deny the jammer this opportunity to confirm his effectiveness, the communication system can be designed to change operating frequency periodically. An alternative or supplementary tactic is to relocate one or more elements of a disrupted communication network to make best use of terrain. The goal of the relocation is to establish a line-of-sight path between the transmitters and receivers and, if the jammer's location is known, to mask the receivers from the jammer by means of terrain obstacles.

Multifrequency transmissions by the communicators make it difficult for the jammer to obtain accurate estimates of the operating frequencies and the locations of the communicators. Rapid frequency changes (fast frequency hopping) preclude the effectiveness of jamming by means of a repeater, a technique often used in radar. If the communicators store, compress, and rapidly transmit all messages, the difficulties of the jammer are further increased.

Jamming of Analog Communications

Jamming effectiveness against analog communications is not dependent upon a similarity between the intended signal and the jamming waveforms. An amplitude-modulated (AM) jamming waveform can be just as effective as more complicated waveforms against AM, phase-modulation (PM), and frequency-modulation (FM) systems. An unmodulated carrier is often a satisfactory choice for jamming PM and FM systems.

Although the bandwidth of the initial bandpass filter may be greater in PM and FM receivers than in a corresponding AM receiver, it is equally important for the jammer to accurately estimate the receiver center frequencies in all three cases. As the jamming power is increased, angle-modulation systems and noncoherent AM systems are susceptible to sudden disruptions due to well-known threshold effects. When the jamming power is so great that the receiver responds to the jamming rather than to the intended signal, the receiver is said to have been "captured." Generally, complete disruption of angle-modulation systems requires less power than complete disruption of AM systems.

The introduction of jamming which resembles bandlimited white Gaussian noise is often more effective against analog and digital communications than introducing an angle-modulated jamming signal of equal power. However, angle-modulated waveforms are much easier to produce than facsimiles of Gaussian processes.

Jamming of Digital Communications

There are two basic ways in which a digital communication system is disrupted by jamming. Either the bit error rate is increased to an intolerable level or the synchronization system is upset. In general, an unacceptably high bit error rate results when the jamming power which passes through the receiver is comparable in magnitude to the intended signal power. Loss of synchronization can result when either the bit synchronization or frame synchronization is destroyed. Restoration of synchronization after it has been lost usually occurs within several bits or frames. However, certain types of enciphered communication systems are particularly vulnerable to high-powered pulsed jamming which causes repeated loss of synchronization.

It is usually advantageous, in attempting to disrupt digital communications, to concentrate the jamming energy in short pulses. The reason is that only a relatively small fraction of the transmitted bits have to be received erroneously to render the message unintelligible. Pulsed jamming signals can cause a substantial increase in the bit error probability. The optimal pulse duration for effective jamming is proportional to the pulse repetition period and the jamming power spectral density, and is inversely proportional to the energy per bit of the intended transmission at the communication receiver.

The bit errors induced by pulsed jamming are clustered. Suppose the communication system employs error-correcting codes. If the jamming pulse duration is comparable to the time interval of an encoded word, the error-correcting coding will not be able to decrease the word error rate significantly.

To reduce the clustering of bit errors, data bits from various words can be interleaved before transmission. Interleaving may be mechanized by permuting the order of a finite block of digits. The block duration should be chosen to exceed the estimated maximum jamming pulse repetition period. Although the received bit error rate is unaltered by this tactic, error-correcting codes will eliminate many of the word errors in the final receiver output.

Cryptographic Considerations

Cryptography is employed when hostile personnel have the technical capability of intercepting and correctly interpreting a message. The effectiveness of modern cryptographic techniques is such that the enemy often loses the option of listening to communications. However, enciphered messages are more easily jammed than those that are not.

Most practical cryptographic digital communications use encipherment, which consists of the substitution of fixed-length groups of bits for fixed-length plaintext groups. Enciphered systems possess high-speed processing and easy modification capabilities.

In any digital communication system, the transmitted bits and words have certain error rates. Except for independently-keyed systems, encipherment causes these error rates to increase if other system parameters remain unchanged. The characteristic increase of the bit errors in most enciphered systems is called error extension.

Although systems with independently-keyed ciphers do not exhibit error extension, they are usually more susceptible to synchronization loss due to pulsed jamming than other enciphered systems. Furthermore, data-independent keys must be frequently changed to maintain security.

The introduction of cryptographic devices into a communication system causes a performance degradation, an increase in jamming susceptibility, a decrease in reliability, and an increase in cost. Thus, cryptographic devices should not be used unless complete message security is mandatory. In addition to encipherment, there is an inherent scrambling of information which results from the multiplexing of data bits, error coding bits, and synchronization bits. Furthermore, even if the various data bits can be unscrambled, the interpretation and use of the data present a formidable problem.

Concealment

An enemy may seek to intercept communications for a variety of reasons including surveillance, tracking, locating, listening, or establishing a jamming target. Directional antennas help to conceal the existence of communications from the enemy. However, there are constraints on the degree of directionality which can be designed into an antenna to be used in the battlefield. An important constraint is the need to keep the antenna small to help hide it from sight.

Since the antenna beam angle can be decreased by the use of a smaller wavelength as well as by a larger antenna, millimeter or even optical frequencies are often viable alternatives to radio frequencies. The decision to use smaller wavelengths is tempered by such things as

costs, available power, and propagation properties. The shorter wavelengths are in general attenuated more than longer wavelengths and are more easily blocked by obstructions in their path. Furthermore, if the beam width is exceedingly narrow, it is more difficult to keep it centered on another station of the communications net.

Spread-spectrum systems conceal the transmitted waveform by distributing its energy nearly uniformly over a wide bandwidth. The most widely used spread-spectrum methods are pseudonoise modulation, frequency hopping, and hybrids of these two methods. Spread-spectrum systems are particularly useful for reducing the impact of narrowband jamming.

The processing gain, which is the ratio of the spread-spectrum bandwidth to the message bandwidth, is a parameter of central importance in assessing the performance of a pseudonoise modulation system. This parameter determines the degree to which the system resists the degrading effects of jamming on the bit error rate.

Adaptive Antennas and Noise Cancellation

In recent years, various adaptive antenna beamforming and noise-cancelling systems have been developed. These systems are designed to reduce the impact of jamming energy which enters a receiver through the sidelobes or the mainlobe of its antenna radiation pattern, while still allowing reception of an intended transmission.

In the single-loop sidelobe canceller, the primary and reference signals are the outputs of two separate antennas which are steered in the directions of the intended transmission and the jamming, respectively. It is intended that the reference signal should provide an estimate of the interference. After suitable processing, this estimate is subtracted from the primary signal, which contains both the intended signal and interference. As a result, the interference is reduced or eliminated by cancellation.

The signal-to-jamming ratio at the output of the sidelobe canceller is inversely proportional to the signal-to-jamming ratio at the reference input. Consequently, the output signal distortion is small when the signal power at the reference antenna is relatively low.

Optical Fibers

Recent advances in optical fiber technology have made optical communication systems both feasible and attractive in certain communication warfare environments. Because optical fibers do not emit a significant amount of electromagnetic energy, they are very effective in preventing the detection and interception of communications by an opponent.

Tapping is more difficult than it is for an electrical cable. Since ambient electromagnetic energy does not interfere significantly with the propagation of optical waves in fibers, communication by means of optical fibers is nearly invulnerable to jamming. Other advantages of optical fibers are the light weight, resistance to fire, lack of "cross-talk" among fibers, and freedom from short circuits. Although it may not be necessary in many military communication systems, optical fibers can carry a much higher message density than metallic conductors of comparable dimensions. For military applications, the major disadvantage of optical fibers relative to ordinary electrical cables appears to be the difficulty of rapidly repairing damaged fibers.

1. INTRODUCTION

Communication warfare is an element of warfare that pits potential communicators against hostile personnel who seek to intercept and/or disrupt the communications. As recently as World War II, communication systems were rarely jammed, for it was more profitable to listen to enemy communications. Today, the development of covert communication techniques has severely curtailed the possibility of intercepting and interpreting communications. Thus, it seems inevitable that military communications in the battlefield will be forced to operate in a jamming environment.

In order not to waste available power, the potential jammer must first intercept the communications and perhaps locate the receivers. Even if special measures are not employed by the communicators, interception of communications is generally more difficult than interception of radar because the communication energy is usually not directed toward the jammer and the transmitted power is low compared with radar. Assuming that the presence of the communications has been established, the jammer faces a situation different from the radar case. Although the communication system uses relatively low power, the jamming signal must compete with a transmitted signal traveling a one-way path, not the two-way path of radar. The jammer is usually farther from the communication receiver than the communication transmitter is, while in the radar case the jammer is often at a distance from the radar system comparable to the length of the return path of the radar signal. Although the jammer can limit the range of a communication system, there is still some range within which communication is possible.

In assessing the potential effectiveness of jamming, it is useful to calculate a signal-to-interference ratio at the communication receiver. Figure 1 illustrates the geometric configuration, where D_T is the distance between the transmitter and receiver, and D_J the distance between the jammer and the receiver. The average power (P_1) of the desired signal at the input of the communication receiver is

$$P_1 = \frac{P_T' G_{TR} G_{RT} \lambda^2}{(4\pi)^2 D_T^2 L_{TR}} , \qquad (1)$$

where P_T is the average transmitter power, G_{TR} is the gain of the transmitter antenna in the direction of the receiver, G_{RT} is the gain of the receiver antenna in the direction of the transmitter, λ is the wavelength, and L_{TR} represents propagation and equipment losses. A similar expression can be written for the power at the receiver antenna due to the jammer. However, the amount of jamming power which reaches the demodulator may be reduced by two factors. First, there is a polarization loss due to the fact that the jammer may not be emitting

radiation with the appropriate polarization. This relative polarization loss may be described by a coefficient p, which has the range $0 \leq p \leq 1$. A second jamming power reduction may be caused by the receiver bandpass filtering. The effect of this filtering usually may be described by a function $f(B_R, B_J)$, where B_R is the bandwidth of the effective receiver bandpass filter, and B_J is the bandwidth of the jamming signal. If the entire jamming spectrum is included in the receiver passband we may write

$$f(B_R, B_J) = 1, \quad B_J \subset B_R \quad . \tag{2a}$$

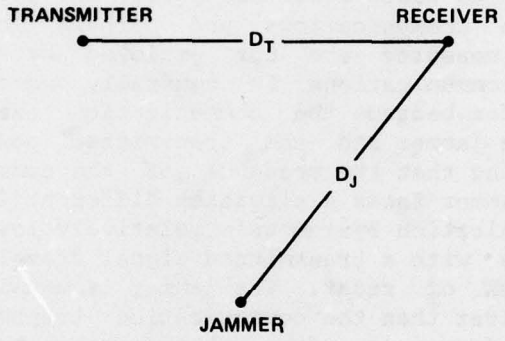


Figure 1. The geometry of communication warfare.

If the jamming spectrum includes the entire receiver passband,

$$f(B_R, B_J) = \frac{B_R}{B_J}, \quad B_R \subset B_J \quad . \tag{2b}$$

The net jamming power affecting the receiver is

$$P_2 = \frac{P_J G_{JR} G_{RJ} \lambda^2 p f(B_R, B_J)}{(4\pi)^2 D_J^2 L_{JR}}, \tag{3}$$

where P_J is the average jamming power, G_{JR} is the gain of the jamming antenna in the direction of the receiver, G_{RJ} is the gain of the receiver antenna in the direction of the jammer, and L_{JR} represents propagation and equipment losses. It has been assumed that the average wavelength of the jamming signal is approximately equal to that of the intended signal.

At the communication receiver, the environmental noise power is equal to kT_eB_R, where k is Boltzmann's constant and T_e is the effective noise temperature. The total interference power is the sum of the environmental power and the jamming power. Thus, the signal-to-interference ratio is

$$S/I = \frac{P_1}{P_2 + kT_eB_R} \quad . \tag{4}$$

If the jamming is to be effective, it is generally necessary that $P_2 >> kT_eB_R$. Making this assumption, we obtain

$$S/I \simeq \frac{P_1}{P_2} = \left[\frac{G_{TR}G_{RT}L_{JR}}{G_{JR}G_{RJ}L_{TR}f(B_R,B_J)p}\right]\left(\frac{P_T}{P_J}\right)\left(\frac{D_J}{D_T}\right)^2 \quad . \tag{5}$$

The term within brackets is usually much greater than unity. Although equation (5) indicates that S/I varies as the square of the distance ratio, D_J/D_T, this variation is attained only if the communication system elements and the jammer are airborne and atmospheric attenuation is negligible. Otherwise, the loss factors, which are measures of the deviations from ideal free-space performance, may be functions of the distances. If both the communication system elements and the jammer are on the ground and we consider the curvature of the spherical earth, the relative dielectric constant, antenna heights, presence of obstacles, and other propagation effects, then S/I varies as the fourth or larger power of the distance ratio.[1]

For acceptable communication system performance, S/I must exceed some minimum level that is determined by the nature of the system. For example, an acceptable bit error rate for a digital communication system operating in bandlimited white Gaussian noise usually requires that

$$\frac{E_b}{N_0} > C \quad , \tag{6}$$

---

[1] *L. E. Follis and R. D. Rood, Jamming Calculations for FM Voice Communications, Electronic Warfare (November/December 1976), 33-40.*

where E_b is the energy per bit, $N_0/2$ is the noise power spectral density, and C is a constant. We assume that the background noise power is negligible compared to the jamming power. If the jamming signal spectrum is appoximately flat over the receiver passband, then we can define an effective interference power spectral density by $N_I B_R = P_2$. In terms of power, $E_b = P_1 T$, where T is the bit period. Then, successful digital communication is possible if

$$\frac{E_b}{N_I} \simeq \frac{P_1 B_R T}{P_2} > C, \quad P_2 >> kT_e B_R \quad . \tag{7}$$

Substituting equation (5) into the above, we see that the required transmitter power is determined by

$$P_T > CP_J \left(\frac{D_T}{D_J}\right)^2 \left[\frac{G_{JR} G_{RJ} L_{TR} f(B_R, B_J) p}{G_{TR} G_{RT} L_{JR} B_R T}\right]. \tag{8}$$

Note that if equation (2b) is applicable, the right-hand side of equation (8) is independent of B_R. Of course, equation (8) can be inverted if it is desired to express the required distances or jamming power in terms of the other quantities.

Ordinarily, the jammer cannot ascertain the effectiveness of the jamming. However, effective jamming may force the communication system to change the operating frequency. If the jammer can detect this change in frequency, he has an important indication that the jamming is indeed disrupting communications. The jammer may then attempt to change the center frequency of the jamming signal accordingly.

In order to deny the jammer this opportunity to confirm his effectiveness, the communication system can be designed to change operating frequency periodically. An alternative or supplementary tactic is to relocate one or more elements of a disrupted communication network to make best use of terrain. The goal of the relocation is to establish a line-of-sight path between the transmitters and receivers and, if the jammer's location is known, to mask the receivers from the jammer by means of terrain obstacles.

Multifrequency transmissions by the communicators make it difficult for the jammer to obtain accurate estimates of the operating frequencies and the locations of the communicators. Rapid frequency changes (fast frequency hopping) preclude the effectiveness of jamming by means of a

repeater, a technique often used in radar. If the communicators store, compress, and rapidly transmit all messages, the difficulties of the jammer are further increased.

If the communication frequencies can be accurately estimated, narrowband jamming can be employed against the communicators. This type of jamming not only allows economical use of power, but also makes it easy for the jammer to avoid jamming his own communication systems. If frequency-estimation equipment is not used, or if accurate frequency estimation is impossible because of rapid frequency changes or other unfavorable conditions, the jammer can employ wideband jamming. In this case, the jamming energy is spread over large spectral regions to increase the probability that some jamming energy will interfere with the enemy communications.

A result of information theory is that the most destructive kind of additive noise in a communication channel is white Gaussian noise.[2] Thus, it is desirable for a jammer to produce a facsimile of bandlimited white Gaussian noise in the passband of the jammed receiver. However, in practice it is difficult to synthesize a waveform with the large random voltage swings of true bandlimited white Gaussian noise. To the extent that the jamming can be modeled as white Gaussian noise, well-known theoretical formulas can often be used to determine the effectiveness of the jamming in degrading the signal-to-interference ratio and system performance.

Non-Gaussian jamming waveforms usually are studied through computer simulations. However, in certain cases, an approximate mathematical analysis can be accomplished. Although such analyses are necessarily limited in scope, they provide valuable insight into the general characteristics of jamming and measures to defeat it. In the next two sections, examples of the jamming of analog and digital communication systems are analyzed.

2. ANALOG COMMUNICATION SYSTEMS

In the analog examples of this section, we shall be particularly interested in determining the validity of the maxim that the most effective type of jamming signal is one that uses the same type of modulation as the intended signal.

---

[2] *N. M. Blachman, Noise and its Effects on Communication, McGraw-Hill (1966).*

We consider a general transmitted waveform, which includes amplitude-modulation (AM), phase-modulation (PM), and frequency-modulation (FM) waveforms as special cases. This waveform is

$$X_1(t) = A_1(t) \cos \left[\omega_1 t + \phi_1(t)\right] \quad , \tag{9}$$

where $A_1(t)$ is the amplitude modulation, $\phi_1(t)$ is the angle modulation, and ω_1 is the carrier frequency. The receiver possesses an initial bandpass filter which passes $X_1(t)$ with negligible distortion. A general form for a jamming waveform may be written as

$$X_2(t) = A_2(t) \cos \left[\omega_2 t + \phi_2(t)\right] \quad . \tag{10}$$

If the amplitude or angle modulation or both are generated by noise, $A_2(t)$ or $\phi_2(t)$ or both may be regarded as sample functions of stochastic processes. It is assumed that ω_2 is sufficiently close to ω_1 and the modulations are such that $X_2(t)$ passes the receiver bandwidth filter with negligible distortion. Alternatively, we may view $X_2(t)$ as the description of the jamming waveform at the output of the receiver bandpass filter.

Throughout the subsequent analysis, we shall neglect the effect of thermal noise for simplicity. Consequently, the signal at the output of the bandpass filter is $X(t) = X_1(t) + X_2(t)$. Using trigonometric identities to expand the cosine term of equation (10), we obtain

$$X(t) = \left[A_1 + A_2 \cos \left(\omega_3 t + \phi_3\right)\right] \cos \left(\omega_1 t + \phi_1\right)$$

$$- A_2 \sin \left(\omega_3 t + \phi_3\right) \sin \left(\omega_1 t + \phi_1\right) \quad , \tag{11}$$

where $\omega_3 = \omega_2 - \omega_1$, $\phi_3 = \phi_2 - \phi_1$, and some of the time-dependencies have been temporarily suppressed. Further trigonometric manipulation yields

$$X(t) = R(t) \cos \left[\omega_1 t + \phi_1(t) + \theta(t)\right] \quad , \tag{12}$$

where

$$R(t) = \left[A_1^2 + A_2^2 + 2A_1A_2 \cos \left(\omega_3 t + \phi_3\right)\right]^{1/2}, \tag{13}$$

and

$$\theta(t) = \tan^{-1}\left[\frac{A_2 \sin\left(\omega_3 t + \phi_3\right)}{A_1 + A_2 \cos\left(\omega_3 t + \phi_3\right)}\right]. \qquad (14)$$

2.1 AM Systems

When an AM signal is transmitted, we have $\phi_1(t) = 0$ and $\phi_3(t) = \phi_2(t)$. The message is carried by $A_1(t)$. Consider a noncoherent system in which the receiver demodulates by means of an envelope detector. An ideal envelope detector produces an output proportional to the instantaneous amplitude $R(t)$ if $\theta(t)$ is slowly varying relative to $\omega_1 t$. Assuming this ideal operation, the envelope detector output is proportional to

$$y(t) = A_1\left[1 + 2\left(\frac{A_2}{A_1}\right)\cos\left(\omega_3 t + \phi_2\right) + \left(\frac{A_2}{A_1}\right)^2\right]^{1/2}. \qquad (15)$$

We expand the square root as a Taylor series in the parameter A_2/A_1 about the origin. Only the first three terms of the expansion are retained. This truncation gives a reasonably small error if $A_1(t) > 2A_2(t)$ for most times of interest. The use of trigonometric identities in our expansion yields

$$y(t) \simeq A_1(t) + A_2(t)\cos\left[\omega_3 t + \phi_2(t)\right] + A_2(t)\left\{\frac{A_2(t)}{4A_1(t)} - \frac{A_2(t)}{4A_1(t)}\cos\left[2\omega_3 t + 2\phi_2(t)\right]\right\}. \qquad (16)$$

If we set $\phi_2(t)$ equal to a constant in equation (16), the effectiveness of the interference is only slightly impaired, except in the unlikely event that $\omega_3 \simeq 0$ and $\phi_2 \simeq 0$. Furthermore, the spectral bandwidth of the jamming signal is decreased, so that the receiver bandpass filter can block less jamming power before it reaches the envelope detector. Thus, an AM signal may be the best choice of jamming waveform, particularly when cost-effectiveness is a criterion. Note that if both $\phi_2(t)$ and $A_2(t)$ are constants, the energy in the interference terms of equation (16) can be reduced by a dc blocking capacitor, especially when $\omega_3 \simeq 0$. Consequently, an unmodulated carrier is not a satisfactory jamming signal.

Ideal coherent demodulation of the intended signal is accomplished when $X(t)$ is multiplied by $2\cos(\omega_1 t + \phi_1)$ and the double-frequency terms are removed by a filter. From equation (11), the output is

$$y(t) = A_1(t) + A_2(t) \cos\left[\omega_3 t + \phi_2(t)\right] \quad . \tag{17}$$

This expression can be compared to equation (16) to see the effects of the highly nonlinear operation of envelope detection. The main problem with coherent demodulation is the need for a locally generated phase-coherent reference. The carrier synchronization system of the receiver is subject to degradation due to jamming. If a carrier component is transmitted, it is susceptible to detection by the enemy, who can then improve the jamming effectiveness once the carrier frequency has been determined.

2.2 PM Systems

When a PM signal is transmitted, we have $A_1(t) = A_1$, a constant. The message is carried by $\phi_1(t)$. The output of an ideal PM discriminator with $X(t)$ as an input is proportional to $\phi_1(t) + \theta(t)$ if the instantaneous amplitude, $R(t)$, is slowly varying as a function of time. If the discriminator is preceded by a bandpass limiter and if $A_1 > 2A_2(t)$ for all times of interest, then the discriminator input has an amplitude which is sufficiently slowly varying for an output proportional to $\phi_1(t) + \theta(t)$ to be a reasonable approximation. From equation (14), the discriminator output is proportional to

$$y(t) = \phi_1 + \tan^{-1}\left[\frac{A_2 \sin\left(\omega_3 t + \phi_3\right)}{A_1 + A_2 \cos\left(\omega_3 t + \phi_3\right)}\right] \quad . \tag{18}$$

We expand the arctangent as a Taylor series in the parameter A_2/A_1 about the origin and retain the first three terms. This truncation gives a reasonably small error if $A_1 > 2A_2(t)$ for all times of interest. Simple trigonometry yields

$$y(t) \approx \phi_1(t) + \frac{A_2(t)}{A_1} \sin\left[\omega_3 t + \phi_3(t)\right]$$

$$- \frac{1}{2}\left[\frac{A_2(t)}{A_1}\right]^2 \sin\left[2\omega_3 t + 2\phi_3(t)\right] \quad . \tag{19}$$

If ω_3 exceeds the message bandwidth, a postdetection filter will remove most of the power in the last two terms. Thus, although the bandwidth of the initial bandpass filter may be greater than in the AM case, it is just as important for the jammer to accurately estimate the receiver center frequency as it is in the AM case. Assuming that ω_3 does not exceed the message bandwidth, there appears to be little loss in jamming effectiveness if $\phi_2(t)$ is a constant, since the interference terms in

equation (19) are still phase modulated by $\phi_1(t)$. (Recall that $\phi_3 = \phi_2 - \phi_1$.) We conclude that a PM jamming waveform offers no particular advantage in the jamming of a PM communication system.

If we set both $A_2(t)$ and $\phi_2(t)$ equal to constants, the jamming effectiveness does not appear to be seriously impaired. Thus, an unmodulated carrier is often a satisfactory jamming signal against a PM communication system, although ineffective against an AM system.

2.3 FM Systems

An FM transmission may be described by equation (9) with $A_1(t) = A_1$, a constant. The message is carried by the derivative of the phase function, which will be denoted by $\phi_1'(t)$. Under the same assumptions made in the PM case, the output of an ideal FM discriminator is proportional to $\phi_1'(t) + \theta'(t)$, where the second term is the derivative of equation (14). A straightforward calculation yields

$$y(t) = \phi_1' + \frac{\left(\omega_3 + \phi_3'\right) A_2 \left[A_2 + A_1 \cos\left(\omega_3 t + \phi_3\right)\right]}{A_1^2 + A_2^2 + 2A_1A_2 \cos\left(\omega_3 t + \phi_3\right)} \quad . \tag{20}$$

As usual, we approximate the second term in this expression by the first three terms of a Taylor series. The result is

$$y(t) \approx \phi_1'(t) + \left[\omega_3 + \phi_3'(t)\right] \frac{A_2(t)}{A_1} \left\{\cos\left[\omega_3 t + \phi_3(t)\right] - \frac{A_2(t)}{A_1} \cos\left[2\omega_3 t + 2\phi_3(t)\right]\right\} . \tag{21}$$

By the same reasoning used in the PM case, we draw analogous conclusions. It is important for the jammer to accurately estimate the receiver center frequency. An FM jamming waveform offers no compelling advantage in the jamming of an FM communication system, nor is the use of an unmodulated carrier unsatisfactory.

Equation (21) indicates that the interference at the receiver output increases with the frequency offset ω_3. Comparing equations (19) and (21) reveals that the jamming is more effective against FM systems than PM systems when the frequency offset is large.

To combat the potentially severe effects of jamming on FM systems, we may adopt the tactics employed against environmental interference.[3] Specifically, we may use a "deemphasis filter" with a bandwidth less than that of the message bandwidth. If the magnitude of this filter decreases as ω^{-1} for large frequencies, the effect of the jamming will not increase with frequency offset. To compensate for the distortion of the message $\phi_1'(t)$ due to the presence of the deemphasis filter, the message should be modified by a "preemphasis filter" before transmission, as shown in figure 2. The preemphasis filter should have a transfer function equal to the reciprocal of the transfer function of the deemphasis filter so that the demodulated message is unchanged.

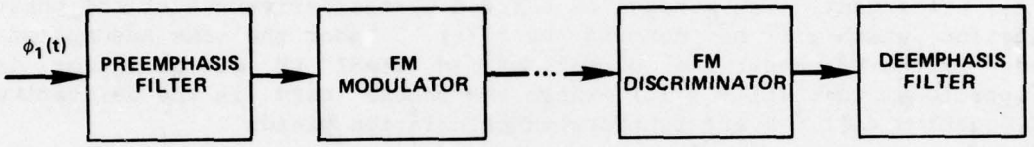


Figure 2. An FM system which resists interference.

Careful design is required when this pair of filters is used. The preemphasis filter amplifies high-frequency spectral components of the message, resulting in an increased bandwidth for the transmitted waveform. If the bandwidth of the receiver is correspondingly increased, the probability that a jamming signal will be intercepted is increased.

Since we have assumed that $A_1(t) > 2A_2(t)$, the performance of all of the above modulation systems in the presence of jamming is excellent. As the jamming power is increased, angle-modulation systems and noncoherent AM systems are susceptible to sudden disruptions due to well-known threshold effects.[4] When the jamming power is so great that the receiver responds to the jamming rather than to the intended signal, the receiver is said to have been "captured." Generally, complete disruption of angle-modulation systems requires less power than complete disruption of AM systems.

---

[3] *R. E. Ziemer and W. H. Tranter, Systems, Modulation, and Noise, Houghton Mifflin (1976).*

[4] *H. Taub and D. L. Schilling, Principles of Communication Systems, McGraw-Hill (1971).*

It has been shown that jamming effectiveness against analog communications is not dependent upon a similarity between the intended signal and the jamming waveforms. An AM jamming waveform can be just as effective as more complicated waveforms against AM, PM, and FM systems. An unmodulated carrier is often a satisfactory choice for jamming PM and FM systems.

3. DIGITAL COMMUNICATION: FREQUENCY-SHIFT KEYING

There are two basic ways in which a digital communication system is disrupted by jamming. Either the bit error rate is increased to an intolerable level or the synchronization system is upset. In this section, the bit error rate degradation due to jamming is investigated in the case of a frequency-shift-keyed (FSK) communication system.

A standard noncoherent FSK receiver is illustrated in figure 3. Coherent FSK, with its added complexity and its practical limitations under fading and jamming conditions, is rarely used. The two possible transmitted signals are represented by

$$s_1(t) = A_1 \cos\left(\omega_1 t\right) ,$$

$$s_2(t) = A_1 \cos\left(\omega_2 t\right) . \qquad (22)$$

The bit period is denoted by T. The frequencies ω_1 and ω_2 are separated by somewhat more than the bandwidth of the receiver bandpass filters shown in the figure. Each of these filters has a bandwidth which is assumed to be large enough that the transmitted pulses are undistorted by the bandpass filters.

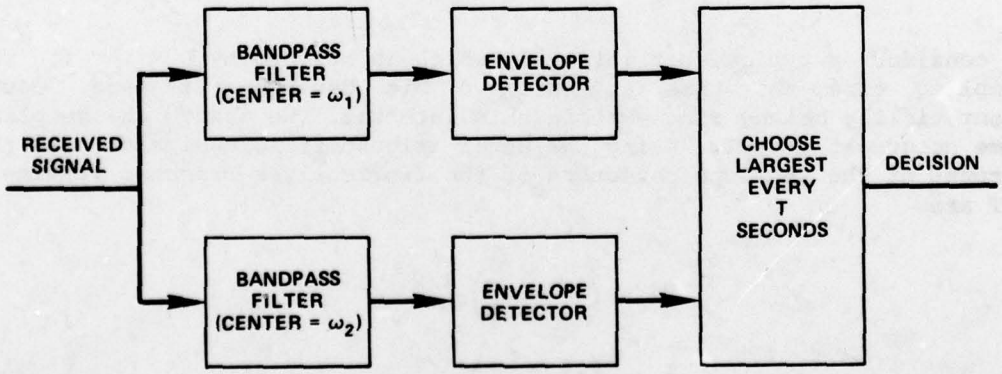


Figure 3. A noncoherent frequency-shift-keyed receiver.

We assume operation in a white Gaussian noise environment. Thus, at the output of the bandpass filters, the bandlimited white Gaussian noise has the narrowband representation,

$$n(t) = n_{ci}(t) \cos\left(\omega_i t\right) - n_{si}(t) \sin\left(\omega_i t\right) , \quad i = 1, 2 , \tag{23}$$

where $n_{ci}(t)$ and $n_{si}(t)$ are Gaussian and independent, and have noise powers equal to N_i. Thus, the noise powers in the two branches of the receiver may be different. We assume that a jamming signal of the form

$$j(t) = A_2(t) \cos\left[\omega_1 t + \phi(t)\right] \tag{24}$$

emerges from the bandpass filter centered at ω_1. No jamming signal is present at the output of the bandpass filter centered at ω_2.

The total signals at the outputs of the two bandpass filters when $s_1(t)$ is transmitted are

$$\begin{aligned} X_1(t) &= A_1 \cos\left(\omega_1 t\right) + A_2 \cos\left(\omega_1 t + \phi\right) \\ &\quad + n_{c1} \cos\left(\omega_1 t\right) - n_{s1} \sin\left(\omega_1 t\right) , \\ X_2(t) &= n_{c2} \cos\left(\omega_2 t\right) - n_{c2} \sin\left(\omega_2 t\right) . \end{aligned} \tag{25}$$

We consider a typical bit interval, which is defined by $0 \leq t \leq T$. The sampling time, the time at which a bit decision is made, could theoretically be any time within this interval. We assume the sampling time occurs at $t = T$. Using the usual trigonometric manipulations, the outputs of the envelope detectors of the two receiver branches at time $t = T$ are

$$\begin{aligned} R_1 &= \left(Z_1^2 + Z_2^2\right)^{1/2} , \\ R_2 &= \left(Z_3^2 + Z_4^2\right)^{1/2} , \end{aligned} \tag{26}$$

where the following definitions are made for notational convenience:

$$Z_1 = A_1 + A_2(T) \cos\left[\phi(T)\right] + n_{c1}(T) \quad ,$$

$$Z_2 = A_2(T) \sin\left[\phi(T)\right] + n_{s1}(T) \quad ,$$

$$Z_3 = n_{c2}(T) \quad ,$$

$$Z_4 = n_{s2}(T) \quad . \tag{27}$$

Since n(t) is assumed to be a zero-mean process, all the noise variables in equation (27) are zero-mean. Denoting an expected value by a bar,

$$\bar{Z}_1 = A_1 + A_2(T) \cos\left[\phi(T)\right] \quad ,$$

$$\bar{Z}_2 = A_2(T) \sin\left[\phi(T)\right] \quad .$$

$$\bar{Z}_3 = \bar{Z}_4 = 0 \quad . \tag{28}$$

Assuming that $A_2(T)$ and $\phi(T)$ are given, the joint probability density function of Z_1 and Z_2 is

$$g_1(z_1,z_2) = \frac{1}{2\pi N_1} \exp\left[-\frac{(z_1 - \bar{Z}_1)^2 + (z_2 - \bar{Z}_2)^2}{2N_1}\right]. \tag{29}$$

If we define $Z_1 = R_1 \cos\Theta$ and $Z_2 = R_1 \sin\Theta$, it follows that the joint probability density function (pdf) of R_1 and Θ is

$$g_2(r_1,\theta_1) = \frac{r_1}{2\pi N_1} \exp\left(-\frac{r_1^2 - 2r_1\bar{Z}_1 \cos\theta_1 - 2r_1\bar{Z}_2 \sin\theta_1 + \bar{Z}_1^2 + \bar{Z}_2^2}{2N_1}\right) ,$$

$$r_1 \geq 0, \ |\theta_1| < \pi \quad . \tag{30}$$

The pdf of the envelope R_1 is obtained by integration over θ_1. First we note that the modified Bessel function of the first kind and zero order satisfies

$$I_0(x) = \frac{1}{2\pi} \int_0^{2\pi} \exp\left[x \cos(u + v)\right] du \tag{31}$$

regardless of the value of v. Consequently, after suitable trigonometric manipulation, the integral of equation (30) over θ_1 can be reduced to

$$f_1(r_1) = \frac{r_1}{N_1} \exp\left(-\frac{\bar{Z}_1^2 + \bar{Z}_2^2 + r_1^2}{2N_1}\right) I_0\left[\frac{\left(\bar{Z}_1^2 + \bar{Z}_2^2\right)^{1/2} r_1}{N_1}\right] ,$$

$$r_1 \geq 0 \quad . \tag{32}$$

In a similar manner, the output at time t = T of the envelope detector in the lower branch of the FSK receiver has the pdf given by

$$f_2(r_2) = \frac{r_2}{N_2} \exp\left(-\frac{r_2^2}{2N_2}\right) , \qquad r_2 \geq 0 \quad . \tag{33}$$

Since $s_1(t)$ has been transmitted, an error occurs if $R_2 > R_1$. Thus, the probability of an error is

$$P(E/1) = \int_0^\infty f_1(r_1) \left[\int_{r_1}^\infty f_2(r_2) dr_2\right] dr_1 \quad . \tag{34}$$

The inner integral is easily evaluated, so we have

$$P(E/1) = \int_0^\infty \frac{r_1}{N_1} \exp\left[-\frac{\left(\bar{Z}_1^2 + \bar{Z}_2^2 + r_1^2\right)}{2N_1} - \frac{r_1^2}{2N_2}\right] I_0\left[\frac{\left(\bar{Z}_1^2 + \bar{Z}_2^2\right)^{1/2} r_1}{N_1}\right] dr_1 \quad . \tag{35}$$

A simple change of variables casts this integral into a form which includes the known definite integral,

$$\int_0^\infty x \exp\left(-\frac{x^2 + \alpha^2}{2}\right) I_0(\alpha x) dx = 1 \quad . \tag{36}$$

After algebraic simplification, equation (35) reduces to

$$P(E/1) = \frac{N_2}{N_1 + N_2} \exp\left[-\frac{\bar{Z}_1^2 + \bar{Z}_1^2}{2(N_1 + N_2)}\right] . \quad (37)$$

The substitution of equation (28) yields

$$P(E/1) = \frac{N_2}{N_1 + N_2} \exp\left[-\frac{A_1^2 + A_2^2 + 2A_1A_2 \cos\phi}{2(N_1 + N_2)}\right], \quad (38)$$

where the explicit dependence on T has been suppressed.

This expression gives P(E/1) for fixed values of $A_2(T)$ and $\phi(T)$. From bit interval to bit interval, these parameters generally will vary in value. If these parameters are modeled as random variables, an aggregate P(E/1) can be calculated by integrating the product of equation (38) and the joint pdf of $A_2(T)$ and $\phi(T)$. To obtain reasonably simple results, we assume that narrowband angle-modulated jamming is present. Thus, we assume that $A_2(t) = A_2(T) = A_2$, a constant. If $\phi(t)$ is nonsynchronous with the carrier frequency of $s_1(t)$, it is logical to model $\phi(T)$ as uniformly distributed from 0 to 2π radians. Thus, the aggregate probability of error, given that $s_1(t)$ was transmitted, is

$$\bar{P}(E/1) = \frac{N_2}{2\pi(N_1 + N_2)} \int_0^{2\pi} \exp\left[-\frac{A_1^2 + A_2^2 + 2A_1A_2 \cos\phi}{2(N_1 + N_2)}\right] d\phi . \quad (39)$$

Using equation (31), this integral can be evaluated, yielding

$$\bar{P}(E/1) = \frac{N_2}{N_1 + N_2} \exp\left[-\frac{A_1^2 + A_2^2}{2(N_1 + N_2)}\right] I_0\left(\frac{A_1A_2}{N_1 + N_2}\right) . \quad (40)$$

The calculation of the probability of bit error, given that $s_2(t)$ was transmitted, follows analogous lines. The probability density functions of the outputs of the envelope detectors are

$$h_1(r_1) = \frac{r_1}{N_1} \exp\left(-\frac{A_2^2 + r_1^2}{2N_1}\right) I_0\left(\frac{A_2 r_1}{N_1}\right) , \quad r_1 \geq 0 , \quad (41)$$

and

$$h_2(r_2) = \frac{r_2}{N_2} \exp\left(-\frac{A_1^2 + r_2^2}{2N_2}\right) I_0\left(\frac{A_1 r_2}{N_2}\right), \quad r_2 \geq 0 \quad . \tag{42}$$

When $s_2(t)$ has been transmitted, an error occurs if $R_1 > R_2$. Thus,

$$P(E/2) = \int_0^\infty h_2(r_2) \left[\int_{r_2}^\infty h_1(r_1) dr_1\right] dr_2 \quad . \tag{43}$$

Substituting equations (41) and (42) into equation (43) we obtain

$$P(E/2) = \int_0^\infty q\left(\frac{A_1}{\sqrt{N_2}}, x\right) Q\left(\frac{A_2}{\sqrt{N_1}}, \frac{\sqrt{N_2}\, x}{\sqrt{N_1}}\right) dx \quad , \tag{44}$$

where we have defined the Rician function,

$$q(\alpha, x) = x \exp\left(-\frac{x^2 + \alpha^2}{2}\right) I_0(\alpha x) \quad , \tag{45}$$

and the Q-function

$$Q(\alpha, \beta) = \int_\beta^\infty q(\alpha, x)\, dx \quad . \tag{46}$$

Integrals of the form of equation (44) are evaluated by Helstrom.[5] The result is

$$P(E/2) = Q\left(\frac{A_2}{\sqrt{N_1 + N_2}}, \frac{A_1}{\sqrt{N_1 + N_2}}\right) - \frac{N_2}{N_1 + N_2} \exp\left[-\frac{A_1^2 + A_2^2}{2(N_1 + N_2)}\right] I_0\left(\frac{A_1 A_2}{N_1 + N_2}\right) . \tag{47}$$

[5] *C. Helstrom, Statistical Theory of Signal Detection, 2nd edition, Pergamon Press (1968).*

Observe that when $s_2(t)$ is transmitted, the probability of error is independent of the phase of the jamming signal. Consequently, equation (47) is the aggregate probability of error, given that $s_2(t)$ is transmitted.

If it is equally likely that either $s_1(t)$ or $s_2(t)$ is transmitted, the total probability of bit error is

$$\bar{P}(E) = \frac{1}{2}\bar{P}(E/1) + \frac{1}{2}\bar{P}(E/2) \quad . \tag{48}$$

Substitution of equations (40) and (47) into equation (48) yields

$$\bar{P}(E) = \frac{1}{2} Q\left[\left(\frac{2P_2}{N_1 + N_2}\right)^{1/2}, \left(\frac{2P_1}{N_1 + N_2}\right)^{1/2}\right] \quad , \tag{49}$$

where $P_1 = A_1^2/2$ is the average power in the transmitted signals and $P_2 = A_2^2/2$ is the average power in the jamming signal. Equations (40), (47), and (49) are useful in the analysis not only of FSK systems, but also of frequency-hopping systems. Plots of $\bar{P}(E)$ as a function of the jamming-to-signal ratio, P_2/P_1, are shown in figure 4.

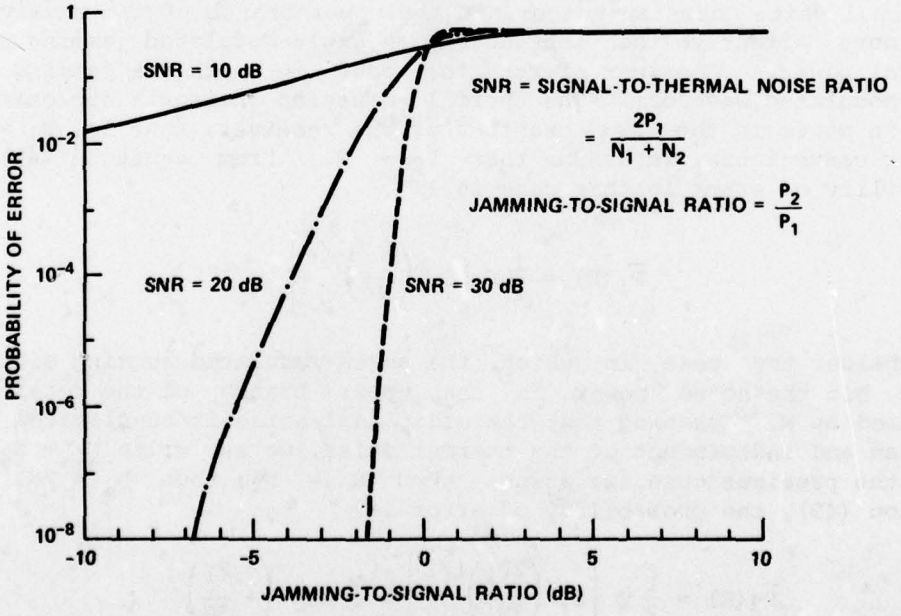


Figure 4. Error probability for frequency-shift-keyed system in presence of angle-modulated jamming entering single branch of receiver.

A special case occurs when the intended and jamming signals have equal power. We use the identity

$$Q(\beta,\beta) = \frac{1}{2} + \frac{1}{2} \exp\left(-\beta^2\right) I_0\left(\beta^2\right) , \tag{50}$$

and set $P_1 = P_2$ and $N_1 = N_2$. Equations (40) and (47) become

$$\overline{P}(E/1) = \frac{1}{2} \exp\left(-\frac{P_1}{N_1}\right) I_0\left(\frac{P_1}{N_1}\right) , \tag{51}$$

and

$$\overline{P}(E/2) = \frac{1}{2} . \tag{52}$$

These equations indicate that an FSK system can be effectively disabled if jamming power comparable to the signal power passes through one of the receiver bandpass filters.

We shall now give an example illustrating that introducing additional white Gaussian noise into the upper branch of the receiver is often more effective than introducing an angle-modulated jamming signal of equal power. Consider first the case in which the jamming is an angle-modulated waveform. The thermal Gaussian noise is approximately equal in power in the two branches of the receiver; that is, $N_1 = N_2 = N$. For convenience, we assume that $P_2 = N$. From equation (49), the probability of error in this case is

$$\overline{P}_1(E) = \frac{1}{2} Q\left[1, \left(\frac{P_1}{N}\right)^{1/2}\right] . \tag{53}$$

Now consider the case in which the angle-modulated jamming signal is absent, but the noise power in the upper branch of the receiver is increased by N. Assuming that the additional noise is bandlimited white Gaussian and independent of the thermal noise, we can write $N_1 = N_2 + N$. As in the previous case, we assume that $N = N_2$; thus, $N_1 = 2N$. From equation (49), the probability of error is

$$\overline{P}_2(E) = \frac{1}{2} Q\left[0, \left(\frac{2P_1}{3N}\right)^{1/2}\right] = \frac{1}{2} \exp\left(-\frac{P_1}{3N}\right) . \tag{54}$$

A comparison of $\overline{P}_1(E)$ and $\overline{P}_2(E)$ as functions of the signal-to-thermal noise ratio, P_1/N, is shown in figure 5. It is concluded that the more effective type of jamming is a facsimile of bandlimited white Gaussian noise, if it can be produced by the jammer.

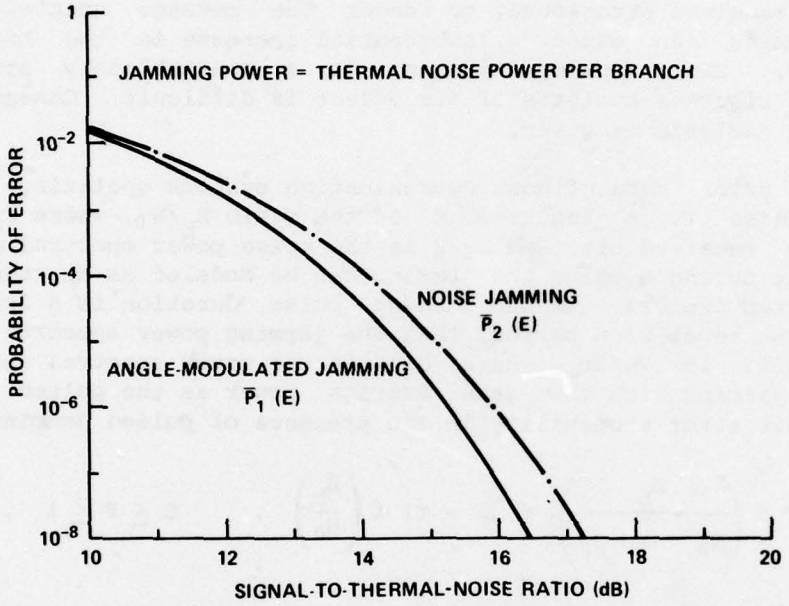


Figure 5. Error probability for frequency-shift-keyed system in presence of two different types of jamming entering single branch of receiver.

In this section, we have assumed that jamming is present in only one of the two receiver branches. A calculation of the probability of bit error when jamming is present in both branches leads to complicated expressions that are not easily interpreted. A calculation assuming that $N_1 = N_2$ has been done by Pettit.[6]

---

[6] *R. Pettit, Error Probability for NCFSK with Linear FM Jamming, IEEE Transactions on Aerospace and Electronic Systems, AES-8 (September 1972), 609-614.*

4. PULSED JAMMING

It is usually advantageous, in attempting to disrupt digital communications, to concentrate the jamming energy in short pulses. The reason is that only a relatively small fraction of the transmitted bits have to be received erroneously to render the message unintelligible. Pulsed jamming can cause a substantial increase in the bit error probability. Since pulsed jamming is a nonstationary stochastic process, a rigorous analysis of its effect is difficult. Consequently, a heuristic analysis is given.

The bit error rate of most communication systems operating in white Gaussian noise is a function f of the ratio E_b/N_0, where E_b is the energy in a received bit, and $N_0/2$ is the noise power spectral density. Suppose that during a pulse the jamming can be modeled as an independent white Gaussian process. If the jamming pulse duration is a fraction r of the pulse repetition period, then the jamming power spectral density during a pulse is $J_0/2r$, where $J_0/2$ is the power spectral density of continuous jamming with the same average power as the pulsed jamming. Thus, the bit error probability in the presence of pulsed jamming is

$$P_E = r\, f\left(\frac{E_b}{N_0 + r^{-1}J_0}\right) + (1 - r)\, f\left(\frac{E_b}{N_0}\right) , \qquad 0 \le F \le 1 . \tag{55}$$

The optimum value of r to maximize P_E, when J_0 is fixed, can be determined from equation (55) by elementary calculus. To obtain a closed-form solution, approximations are necessary. As an example, we consider a differential phase-shift-keyed (DPSK) system. In this case,[3,4]

$$f\left(\frac{E_b}{N_0}\right) = \frac{1}{2} \exp\left(-\frac{E_b}{N_0}\right) . \tag{56}$$

---

[3] *R. E. Ziemer and W. H. Tranter, Systems, Modulation, and Noise, Houghton Mifflin (1976).*

[4] *H. Taub and D. L. Schilling, Principles of Communication Systems, McGraw-Hill (1971).*

If $J_0 >> N_0$, then

$$f\left(\frac{E_b}{N_0 + r^{-1}J_0}\right) \simeq \frac{1}{2} \exp\left(-\frac{rE_b}{J_0}\right). \tag{57}$$

Substituting equations (56) and (57) into equation (55), differentiating with respect to r, and equating to zero, we obtain

$$\exp\left(-\frac{rE_b}{J_0}\right) - \exp\left(-\frac{E_b}{N_0}\right) = \frac{rE_b}{J_0} \exp\left(-\frac{rE_b}{J_0}\right) . \tag{58}$$

Since $J_0 >> N_0$ and $r < 1$, the second term on the left-hand side is much smaller than the first term and can be ignored. It is then a simple matter to obtain

$$r \simeq \frac{J_0}{E_b} \tag{59}$$

as the optimum value if $J_0/E_b \leq 1$. If $J_0/E_b \geq 1$, then $r = 1$ is the optimum choice for the jammer; that is, a continuous jamming waveform should be produced.

The bit errors induced by pulsed jamming are clustered. Suppose the communication system employs error-correcting codes. If the jamming pulse duration is comparable to the time interval of an encoded word, the error-correcting coding will not be able to decrease the word error rate significantly.

To reduce the clustering of bit errors, data bits from various words can be interleaved before tranmission. Interleaving may be mechanized by permuting the order of a finite block of digits. The block duration should be chosen to exceed the estimated maximum jamming pulse repetition period. Although the received bit error rate is unaltered by this tactic, error-correcting codes will eliminate many of the word errors in the final receiver output.

In addition to increasing the bit error rate, pulsed jamming can be the cause of the loss of synchronization in a digital communication system. The susceptibility of the synchronization system is often increased when the data bits are enciphered, as discussed in the next section.

5. CRYPTOGRAPHIC DIGITAL COMMUNICATION

Cryptography is often employed when hostile personnel have the technical capability of intercepting and correctly interpreting a message. The effectiveness of modern cryptographic techniques is such that the enemy often loses the option of listening to communications. However, enciphered messages are more easily jammed than those that are not.

Most practical cryptographic digital communications use encipherment, which consists of the substitution of fixed-length groups of bits for fixed-length plaintext groups. Enciphered systems possess high-speed processing and easy modification capabilities. (Feistal[7] gives a discussion of the fundamentals of cryptography and encipherment.)

There are two basic types of enciphered bit sequences: the stream cipher and the block cipher. The stream cipher is obtained from bit-by-bit encipherment which results when one of a set of binary symbols is added, modulo two, to each bit of plaintext. The complete set of binary symbols or the rule for generating it is called the key. Deciphering is accomplished by adding the key to the corresponding enciphered bit. The more random the key, the more difficult it is for a cryptanalyst to decipher an intercepted cryptogram. A block cipher results from the conversion of m plain bits simultaneously into n enciphered bits. Each of the enciphered bits is a function of all m plain bits. For unambiguous deciphering, it is necessary that $n \geq m$. For ease of automation, it is preferable that $n = m$. Since knowledge of the conversion of one block of bits reveals little or nothing about the conversion of another block, the block cipher can be made secure by employing large values of n. To safeguard against the frequency analysis of block patterns, it is usually necessary that $n \geq 4k$, where k is the length of the enciphered words.

Many electronic cryptographic systems use a stream cipher which incorporates some of the useful aspects of the block cipher. The technique is to use a pseudo-random key which is a function of the plaintext itself. Thus, each enciphered bit is a function of many preceding plain bits. This type of stream cipher is called a data-keyed cipher. A block diagram of a general data-keyed enciphering or deciphering system is shown in figure 6.

---

[7] *H. Feistel, Cryptography and Computer Privacy, Scientific American, 228 (May 1973), 15-23.*

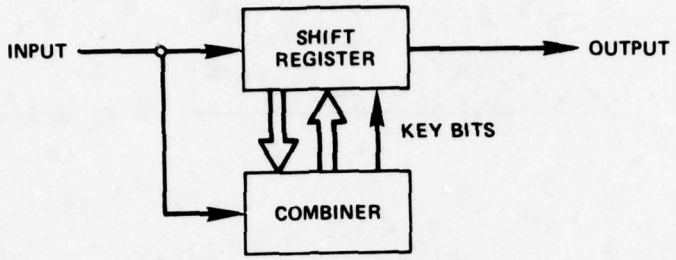


Figure 6. Data-keyed enciphering or deciphering system.

In any digital communication system, the transmitted bits and words have certain error rates. Except for systems using stream ciphers with data-independent keys, encipherment causes these error rates to increase if other system parameters remain unchanged. In block-enciphered systems, each deciphered bit is a function of all the transmitted enciphered bits in the corresponding block. Therefore, a single erroneous received bit is practically certain to cause many erroneous deciphered bits. For the data-keyed system of figure 6, the degradation is due to the presence of the shift register. A received bit error is carried through the shift register, causing additional bit errors down the line. The characteristic increase of the bit errors in block-enciphered and data-keyed systems is called error extension.

We assume that the bit errors at the input of a deciphering system occur independently of each other, and denote the probability of bit error by P_b. As an erroneous bit proceeds through the deciphering system, each of n consecutive bits will be affected. For a stream cipher with a data-independent key, $n = 1$; for a data-keyed or block cipher, $n > 1$. The probability of a word error, P_{cw}, is defined to be the probability of one or more erroneous bits in an output word of k bits emerging from the deciphering system. A measure of the error-rate performance of an enciphered system is obtained by considering ensembles of stream ciphers or block ciphers characterized by a specific value of the parameter n. We indicate the ensemble average of a probability by a bar over the P.

Consider a communication system with a stream cipher. The ensemble-average probability of a word error for the practical case in which $n \geq k$ has been shown to be[8]

[8] *D. J. Torrieri, Cryptographic Digital Communication, IEEE Transactions on Aerospace and Electronic Systems, AES-12 (January 1976), 2-11.*

$$\overline{P}_{cw} = 1 - 2^{-k} + k2^{-k} P_b\left(1 - P_b\right)^{n-1} - \frac{\left(1 - P_b\right)^n \left[\left(1 - P_b\right)^k - 2^{-k}\right]}{1 - 2P_b} , \quad P_b \neq 1/2 ;$$

$$\overline{P}_{cw} = 1 - 2^{-k} , \quad P_b = 1/2 . \tag{60}$$

A simple asymptotic expression is

$$\overline{P}_{cw} \simeq \left[n + k - 2 - 2^{-k}(n - k - 2)\right] P_b , \quad n \geq k . \tag{61}$$

A sufficient condition for the validity of this equation is

$$P_b << (n + k - 2)^{-1} , \quad n + k > 2 . \tag{62}$$

This condition is usually satisfied in practical applications.

A similar expression can be written for a communication system employing a block cipher. We have

$$\overline{P}_{cw} = \left(1 - 2^{-n}\right)^{-1} \left(1 - 2^{-k}\right) \left[1 - \left(1 - P_b\right)^n\right] . \tag{63}$$

Under the condition that

$$P_b << 2(n - 1)^{-1} , \tag{64}$$

we obtain the asymptotic formula

$$\overline{P}_{cw} \simeq \left(1 - 2^{-n}\right)^{-1}\left(1 - 2^{-k}\right)nP_b . \tag{65}$$

Let E_b denote the mean energy of a received bit. A measure of the degradation due to encipherment is the increase in E_b required for a cryptographic system to have the same error rate as the corresponding plaintext system. For ideal *noncoherent* modulation systems, the degradation in decibels has been shown to be[8]

$$D_N = 10 \log_{10} \left[1 - \frac{\ln g(n,k)}{\ln 2P_b} \right], \tag{66}$$

where it is assumed that the asymptotic error rate formulas are valid and we define

$$g(n,k) = n + k - 2 - 2^{-k}(n - k - 2) \tag{67}$$

for stream ciphers and

$$g(n,k) = \left(1 - 2^{-n}\right)^{-1} \left(1 - 2^{-k}\right)n \tag{68}$$

for block ciphers. Equation (66) also serves as an approximation to the degradation in ideal coherent modulation systems. Note that this equation does not depend upon whether the modulation is amplitude, frequency, phase, or quadri-phase shift-keyed. For fixed values of n and k, the degradation due to the presence of a stream cipher equals or exceeds that due to the presence of a block cipher.

When a stream cipher has a data-independent key, n = 1. It follows that

$$\overline{P}_{cw} = 1 - \left(1 - P_b\right)^k \quad , \tag{69}$$

which is the same as the plaintext word error rate or the error rate of the words entering the deciphering system. Thus, there is no degradation due to the propagation of errors in this type of communication system.

---

[8] *D. J. Torrieri, Cryptographic Digital Communication, IEEE Transactions on Aerospace and Electronic Systems, AES-12 (January 1976), 2-11.*

In all the above discussion, it has been tacitly assumed that the synchronization systems operate perfectly. This assumption is usually reasonable for operation in a thermal noise environment, but must be reconsidered in a fading or jamming environment. The operation of communication systems using stream ciphers with data-independent keys, which we call independently-keyed systems, depends upon the perfect alignment of key bits and received bits in the deciphering system. Since the key is generally many frames in length, once misalignment occurs, special measures must be employed to restore synchronization. In contrast, communication systems with data-keyed ciphers maintain alignment of the bits automatically since the key bits are continually produced by the received bits. Synchronization is lost in a data-keyed system whenever the receiver incorrectly identifies the word boundaries. Synchronization is lost in a block-enciphered system whenever the receiver incorrectly identifies the block boundaries. Both data-keyed and block-enciphered systems often can resynchronize automatically as soon as the next frame identification bits are received.

Loss of synchronization can occur when a high-powered burst of energy causes the clock output of a bit synchronizer to skip a pulse or generate an extra pulse. Alternatively, synchronization can be lost when interference causes a sufficient number of frame synchronization bits to be received erroneously. When this event is recognized, an independently-keyed system assumes that a misalignment has occurred and initiates the resynchronization procedure.

Suppose high-powered jamming of pulse duration T_D occurs every T_B seconds during the transmission of independently-keyed ciphers. If a jamming pulse causes a loss of synchronization in the receiver, time is lost while the communication system recognizes the loss of synchronization, initiates the resynchronization procedure, and reestablishes synchronization between the enciphered bits at the receiver and the stored key bits. We shall call this lost time the reacquisition time and denote its average duration by T_R. Since reacquisition cannot be completed until the jamming has ceased, $T_R > T_D$, as illustrated in figure 7. In general, T_R will be a function of T_D. When T_D is sufficiently large, it is reasonable to expect that $T_R \approx T_D + C$, where C is a constant.

During the reacquisition time, the probability of error of the deciphered bits in the receiver is one-half, since the transmitted information has been entirely destroyed. (If the receiver output is set to zero upon recognition of a synchronization loss, the missing bits must be guessed, so the equivalent bit error rate is one-half.) After reacquisition, assuming there is no further loss of synchronization before the occurrence of the next jamming pulse, the bit error probability at the output of the deciphering system becomes P_b, the usual channel bit error rate. In order to ignore the relative time alignment of the bit edges and the jamming pulses, we assume that

$$T_R >> T \quad , \qquad T_B - T_R >> T \quad , \tag{70}$$

where T is the data bit period. It follows that the expected number of bit errors over a pulse period for an independently-keyed system is given by

$$N_I \simeq \left(\frac{T_R}{T}\right)\frac{1}{2} + \left(\frac{T_B - T_R}{T}\right)P_b \tag{71}$$

Suppose the same high-powered pulsed jamming temporarily disrupts a data-keyed system of length n. We shall ignore the possibility of a word synchronization problem initially. (If this problem exists, but no further disruptions occur, normal operation will resume within one or two frames.) For the pulse duration and n - 1 bits following the cessation of the jamming pulse, the bit error probability is one-half. The remaining bits before the next pulse have an error probability of P_{cb}, which is defined to be P_{cw} with k = 1. As seen in figure 7, the relative time alignments of the bit edges and the pulses may be ignored by assuming that

$$T_D + (n - 1)T >> T \quad ,$$

$$T_B - T_D - (n - 1)T >> T \, . \tag{72}$$

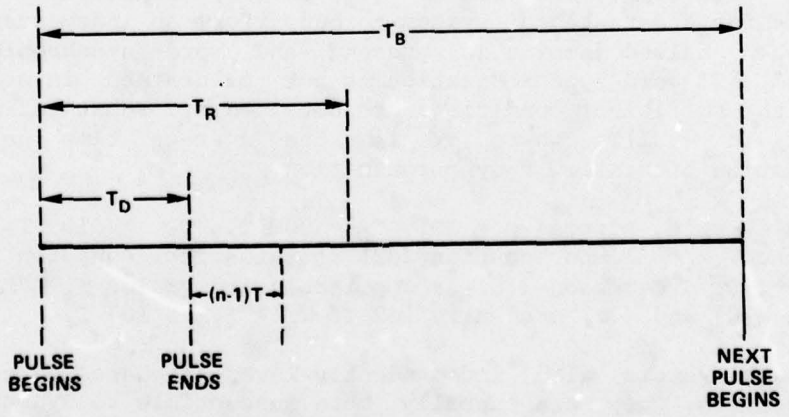


Figure 7. Timing diagram for pulsed jamming of enciphered systems.

It follows that the expected number of bit errors over a pulse period for a data-keyed system is given by

$$N_D \simeq \left[\frac{T_D + (n-1)T}{T}\right]\frac{1}{2} + \left[\frac{T_B - T_D - (n-1)T}{T}\right]\overline{P}_{cb} \quad . \tag{73}$$

Assuming word synchronization is maintained, a data-keyed system has a lower bit error rate than an independently-keyed system if $N_D < N_-$. From equations (71) and (73), we see that this situation exists if

$$T_B < \frac{T_R\left(\frac{1}{2} - P_b\right) - \left[T_D + (n-1)T\right]\left(\frac{1}{2} - \overline{P}_{cb}\right)}{\overline{P}_{cb} - P_b} \quad . \tag{74}$$

In most practical communication systems employing a data-keyed cipher, this inequality can be approximated by

$$T_B < \frac{T_R - T_D - (n-1)T}{2\overline{P}_{cb}}, \quad P_b << \overline{P}_{cb} << \frac{1}{2} \quad . \tag{75}$$

Equations (70), (72), and either (74) or (75) constitute sufficient conditions for a data-keyed system to outperform an independently-keyed system when pulsed jamming is present and word synchronization is maintained. If word synchronization is not maintained in a data-keyed system, the sufficient conditions are obtained by substituting T_F in place of $(n-1)T$, where T_F is the average time until frame identification bits allow resynchronization.

As an example, suppose $n = 101$, $T_D = 900\ T$, $T_R = 10^4\ T$, and $P_b = 10^{-4}$. Since $k = 1$ and equation (62) is satisfied, equation (61) gives $\overline{P}_{cb} \simeq 5.1 \times 10^{-3}$. Equation (75) is applicable and yields $T_B < 0.9 \times 10^6\ T$. Equations (70) and (72) are satisfied if $T_B > 1.1 \times 10^4\ T$.

Although systems with independently-keyed ciphers do not exhibit error extension, they are usually more susceptible to synchronization loss due to pulsed jamming than systems with block or data-keyed ciphers. Furthermore, data-independent keys must be frequently changed to maintain security. Block-enciphered systems are probably slightly less secure and slightly less degraded by pulsed jamming than data-keyed systems.

To reduce the bit error rate and the jamming susceptibility of an enciphered system, error coding can be superimposed on the cipher. Figure 8 illustrates one possible system configuration. The data bits are first enciphered and then encoded; after transmission and reception, the bits are first decoded and then deciphered. If an independently-keyed cipher is employed with error coding, an equally effective system configuration usually results when the inner and outer blocks are interchanged. However, if a data-keyed cipher is used in combination with an error-correcting code, an interchange is inappropriate because of error extension.

Figure 8. Encoding superimposed on encipherment.

The introduction of cryptographic devices into a communication system causes a performance degradation, an increase in jamming susceptibility, a decrease in reliability, and an increase in cost. Thus, cryptographic devices should not be used unless complete message security is mandatory. Even if encipherment is not employed, there is usually an inherent scrambling of information which results from the multiplexing of data bits, error coding bits, and synchronization bits. Furthermore, even if the various types of bits can be unscrambled, the interpretation and use of the data often present a formidable problem.

6. SPREAD-SPECTRUM SYSTEMS

An enemy may seek to intercept communications for a variety of reasons including surveillance, tracking, locating, listening, or establishing a jamming target. Directional antennas help to conceal the existence of communications from the enemy. However, there are constraints on the degree of directionality which can be designed into an antenna to be used in the battlefield. An important constraint is the need to keep the antenna small to help hide it from sight.

Since the antenna beam angle can be decreased by the use of a smaller wavelength as well as by a larger antenna, millimeter or even optical frequencies are often viable alternatives to radio frequencies. The decision to use smaller wavelengths is tempered by such things as cost, available power, and propagation properties. The shorter wavelengths are in general attenuated more than longer wavelengths and are more easily blocked by obstructions in their path. Furthermore, if the beam width is exceedingly narrow, it is more difficult to keep it centered on another station of the communications net.

Spread-spectrum systems conceal the transmitted waveform by distributing its energy nearly uniformly over a wide bandwidth. The most general method of detecting the presence of properly designed spread-spectrum communications is by means of a radiometer, or energy detector. These detectors can be designed by modeling the spread-spectrum signal as a stochastic process and employing statistical communication theory.[5,9]

The most widely used spread-spectrum methods are pseudonoise (PN) modulation, frequency hopping, and hybrids of these two methods. We shall briefly discuss the most important aspects of PN systems with respect to communication warfare. Further information on spread-spectrum systems can be obtained from Dixon[10] and elsewhere.[11] Dixon provides an extensive bibliography on the subject.

A received PN spread-spectrum signal has the form

$$s(t) = Am(t)p(t) \cos \omega t \quad , \tag{76}$$

where A is the amplitude, m(t) is the binary message sequence, and p(t) is a binary pseudo-random sequence. Both m(t) and p(t) take the values +1 or -1. The message bits have a period T, while the pseudo-random bits have a period $\tau = T/n$, where n is a positive integer. The message bit transitions coincide with transitions of the pseudo-random bits. The bandwidth of the received PN signal is on the order of $B_s \simeq 2/\tau = 2n/T$; thus it increases linearly with n.

At the communication receiver, demodulation proceeds as indicated in figure 9. We shall ignore possible synchronization problems. After passage through a wideband filter of bandwidth B_s, the PN signal is multiplied by a local code replica of p(t) to yield $s_1(t) = Am(t) \cos \omega t$ at the input of the narrowband filter. This filter has a bandwidth such that $s_1(t)$ passes with negligible distortion. Since $s_1(t)$ has the form of a PSK signal, the corresponding demodulator will extract m(t).

---

[5] *C. Helstrom, Statistical Theory of Signal Detection, 2nd edition, Pergamon Press (1968).*

[9] *H. L. Van Trees, Detection, Estimation, and Modulation Theory, III, Wiley (1971).*

[10] *R. C. Dixon, Spread Spectrum Systems, Wiley (1976).*

[11] *Spread Spectrum Communications, National Technical Information Service, AD-766-914 (1973).*

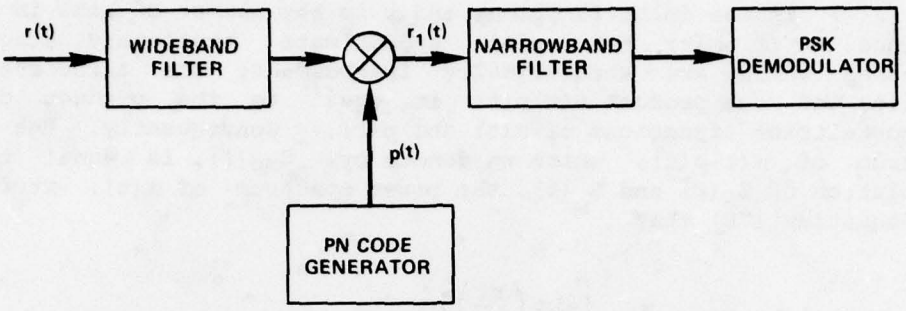


Figure 9. PN spread-spectrum receiver.

The form of equation (76) suggests a method by which s(t) can be intercepted. Suppose s(t) enters a wideband receiver and is squared. Since $m^2 = p^2 = 1$, the output of the squaring device is proportional to

$$s^2(t) = A^2 \cos^2 \omega t = \frac{A^2}{2} + \frac{A^2}{2} \cos 2\omega t \quad . \tag{77}$$

If $s^2(t)$ is applied to an integrator, "energy detection" of the spread-spectrum signal is possible.[12] The double-frequency term can be detected and the carrier frequency can be estimated by means of a phase-locked loop. Although detection or tracking might be accomplished in this manner, the interceptor cannot demodulate s(t) without knowledge of p(t).

It should be noted that p(t) is not necessarily a cryptographically secure code. Frequently p(t) is designed to facilitate code generation or synchronization. If cryptographic integrity is desired, m(t) can be enciphered before multiplication with p(t).

The power spectrum of p(t) is given by

$$S_p(f) = \frac{k+1}{k^2} \left(\frac{\sin \pi f \tau}{\pi f \tau} \right)^2 \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \delta\left(f - \frac{i}{k\tau} \right) + \frac{1}{k^2} \delta(f), \tag{78}$$

[12] *H. Urkowitz, Energy Detection of Unknown Deterministic Signals, Proceedings of the IEEE, 55 (April 1967), 523-531.*

where $\delta(\ )$ is the delta function, and k is the number of bits in the PN sequence.[11] If m(t) and p(t) approximate stationary stochastic processes which are statistically independent, the autocorrelation function of the product m(t)p(t) is equal to the product of the autocorrelation functions of m(t) and p(t). Consequently, the power spectrum of m(t)p(t), which we denote by $S_{mp}(f)$, is equal to the convolution of $S_p(f)$ and $S_m(f)$, the power spectrum of m(t). It follows from equation (78) that

$$S_{mp}(f) \simeq \frac{k+1}{k^2} \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \left[\frac{\sin\left(\frac{\pi i}{k}\right)}{\frac{\pi i}{k}} \right]^2 S_m\left(f - \frac{i}{k\tau}\right) + \frac{1}{k^2} S_m(f) \quad . \tag{79}$$

From the above, we see that $B_m \geq 2/k\tau$ is required if the spectrum of m(t)p(t) is to be approximately flat. Thus, a necessary condition for communication concealment from spectrum analysis is $k \geq B_s/B_m$.

The bit error probability of an ideal PSK system operating in white Gaussian noise is

$$P_E = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right) \quad , \tag{80a}$$

where the complementary error function is defined by

$$\operatorname{erfc} x = \frac{2}{\sqrt{\pi}} \int_x^{\infty} \exp(-x_1^2) dx_1 \quad . \tag{80b}$$

E_b is the energy per bit and $N_0/2$ is the noise power spectral density.[4] Suppose that a jamming signal accompanies the signal at the receiver. Then the received signal is

$$r(t) = s(t) + j(t) + n(t) \quad , \tag{81}$$

where j(t) represents the jamming and n(t) represents the thermal noise. From equation (76), the input to the narrowband filter is

---

[4] *H. Taub and D. L. Schilling, Principles of Communication Systems, McGraw-Hill (1971).*

[11] *Spread Spectrum Communications, National Technical Information Service, AD-766-914 (1973).*

$$r_1(t) = Am(t) \cos \omega t + j(t)p(t) + n(t)p(t) \quad . \tag{82}$$

The presence of the factor p(t) in the last two interference terms ensures that the energies of both terms are spread over a bandwidth at least equal to B_s, and possibly over a bandwidth of $2B_s$, since j(t) and n(t) could have energy over the entire bandwidth of the wideband filter. In order to employ equation (80a) to determine an approximate formula for the bit error probability of a PN system, we make some simplifying assumptions which are approximately valid in the majority of practical cases. We assume that the interference entering the narrowband filter, $i(t) = j(t)p(t) + n(t)p(t)$, can be approximated as a stationary Gaussian process. Since $B_m << B_s$, it is reasonable to assume further that the power spectral density of i(t) is nearly constant over the bandwidth of the narrowband filter. Thus, once this power spectral density is calculated at the center frequency of the two filters, we may substitute it in place of $N_0/2$ in equation (80a) to determine the bit error probability of a PN system.

We assume that the PN code is sufficiently long that the pseudorandom p(t) is well approximated as a random binary sequence (see Papoulis[13]). Then, the power spectral density, $S_{np}(f)$, of the product n(t)p(t) is equal to the convolution of the power spectral densities of n(t) and p(t). A straightforward calculation shows that over the narrowband filter passband, $S_{np}(f) \simeq N_0/2$, the power spectral density of the bandlimited white noise emerging from the wideband filter.

We assume that j(t) can be modeled as a stationary stochastic process. The power spectral density, $S_{jp}(f)$, of the product j(t)p(t) is equal to the convolution of the power spectral densities of j(t) and p(t). If j(t) has a flat spectrum over B_s, then over the narrowband filter passband, $S_{jp}(f) \simeq J/2B_s$, where J is the total jamming power emerging from the wideband filter. Suppose that $j(t) = A_1 \cos(\omega_1 t + \phi)$, where ϕ is a uniformly distributed random variable. If the jamming frequency, ω_1, is near the center frequency of the wideband and narrowband filters, a straightforward calculation yields $S_{jp}(f) \simeq A_1^2\tau/4 \simeq J/B_s$ over the narrowband filter passband. Thus, the power spectral density of the product j(t)p(t) is $cJ/2B_s$, where $c \simeq 1$ for wideband barrage jamming and $c \simeq 2$ for center-frequency, unmodulated-carrier jamming. When narrowband jamming which is offset from the center frequency of the filters is present, we have $c < 2$.

---

[13] *A. Papoulis, Probability, Random Variables, and Stochastic Processes, McGraw-Hill (1965), 294, 341.*

The total interference power spectral density at the narrowband filter input is $N_0/2 + cJ/2B_s$. The energy per bit may be expressed as $E_b = P_s T$, where P_s is the average power in the intended transmission. Thus, equation (80a) implies that the bit error probability for an ideal PN system is given by

$$P_E = \frac{1}{2} \operatorname{erfc} \left[\sqrt{\left(\frac{B_s}{B_m}\right)\left(\frac{P_s B_m T}{cJ + N_0 B_s}\right)} \right] . \tag{83}$$

The product $B_m T$ is a constant usually assumed to equal one or two. The ratio B_s/B_m is known as the processing gain because an increase in this ratio is helpful against narrowband jamming and wideband jamming for which J is fixed. Increasing the processing gain by increasing B_s is not helpful against wideband jamming for which J increases proportionately with B_s.

If J is sufficiently large, P_E will be unsatisfactorily large despite the processing gain. If j(t) is an unmodulated carrier, a phase-locked loop can be swept through B_s to acquire its frequency. The jamming waveform can then be subtracted from the received signal to eliminate this type of interference.

7. ADAPTIVE ANTENNA SYSTEMS

In recent years, various adaptive antenna beamforming and noise-cancelling systems have been developed. These systems are designed to reduce the impact of jamming energy which enters a receiver through the sidelobes or the mainlobe of its antenna radiation pattern, while still allowing reception of an intended transmission. Gabriel[14] and Widrow et al (1967, 1975)[15,16] should be consulted for detailed discussions of the various adaptive antenna techniques. In this section, an illustrative example of an adaptive antenna system is presented as an introduction to the fundamental concepts.

Figure 10 shows a simplified version of a single-loop sidelobe canceller. The primary and reference signals are outputs of two separate antennas or two different groups of elements in a phased-array antenna. It is intended that the reference signal should provide an

---

[14] *W. F. Gabriel, Adaptive Arrays--An Introduction, Proceedings of the IEEE, 64 (February 1976), 239-272.*

[15] *B. Widrow, P. E. Mantey, L. J. Griffiths, and B. B. Goode, Adaptive Antenna Systems, Proceedings of the IEEE, 55 (December 1967), 2143-2159.*

[16] *B. Widrow et al, Adaptive Noise Cancelling: Principles and Applications, Proceedings of the IEEE, 63 (December 1975), 1692-1716.*

estimate of the interference in the primary signal. After suitable processing, this estimate is subtracted from the primary signal, with the result that the interference is reduced or eliminated by cancellation.

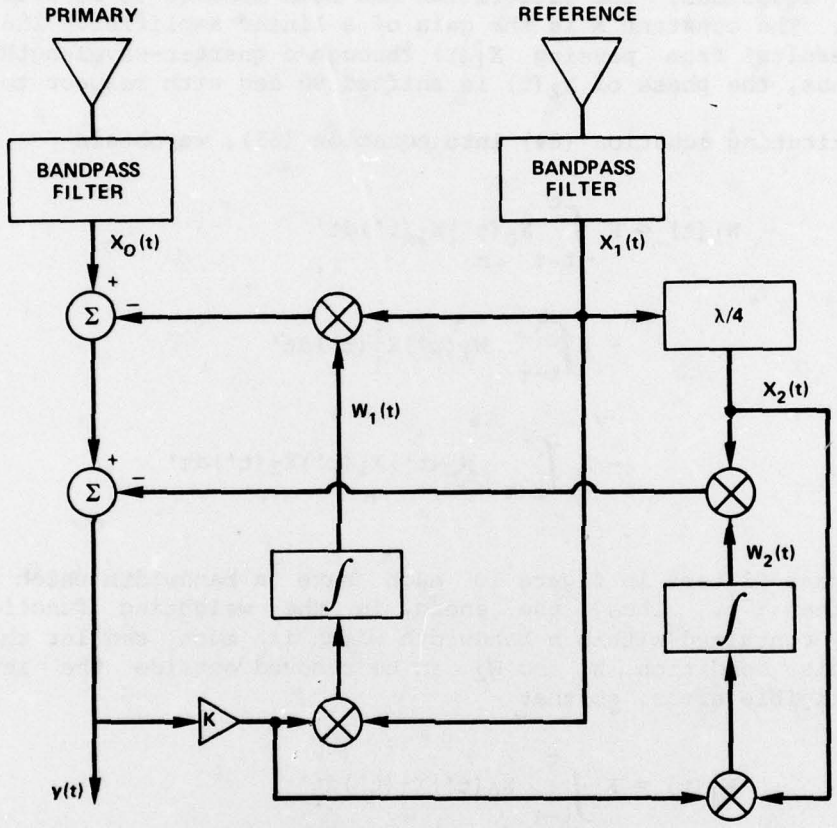


Figure 10. A single-loop sidelobe canceller.

We assume that the primary antenna has been steered in the direction of the intended transmission. The reference antenna may point in the direction of the jamming or may be non-directional. From the block diagram, the output, $y(t)$, and the weighting functions, $W_1(t)$ and $W_2(t)$, are given by

$$y(t) = X_0(t) - W_1(t)X_1(t) - W_2(t)X_2(t) \quad , \tag{84}$$

$$W_1(t) = K \int_{t-\tau}^{t} y(t')X_1(t')dt' \quad , \tag{85}$$

$$W_2(t) = K \int_{t-\tau}^{t} y(t')X_2(t')dt' \quad . \tag{86}$$

In these equations, the integration has been assumed to be over a time period τ. The constant K is the gain of a linear amplifier. The signal $X_2(t)$ results from passing $X_1(t)$ through a quarter-wavelength delay line. Thus, the phase of $X_2(t)$ is shifted 90 deg with respect to $X_1(t)$.

Substituting equation (84) into equation (85), we obtain

$$\begin{aligned} W_1(t) = K &\int_{t-\tau}^{t} X_0(t')X_1(t')dt' \\ &- K\int_{t-\tau}^{t} W_1(t')X_1^2(t')dt' \\ &- K\int_{t-\tau}^{t} W_2(t')X_1(t')X_2(t')dt' \quad . \end{aligned} \tag{87}$$

The bandpass filters in figure 10 each have a bandwidth which is much smaller than τ^{-1}. Thus, the energy in the weighting functions is primarily contained within a bandwidth which is much smaller than τ^{-1}. Under this condition, W_1 and W_2 can be removed outside the integrals with negligible error, so that

$$\begin{aligned} W_1(t) = K &\int_{t-\tau}^{t} X_0(t')X_1(t')dt' \\ &- KW_1(t)\int_{t-\tau}^{t} X_1^2(t')dt' \\ &- KW_2(t)\int_{t-\tau}^{t} X_1(t')X_2(t')dt' \quad . \end{aligned} \tag{88}$$

We now assume specific waveforms for $X_0(t)$ and $X_1(t)$. The intended transmission received by the primary antenna is denoted by s(t) and the jamming signal which passes through the bandpass filter is denoted by j(t). Thus, if we ignore the thermal noise,

$$X_0(t) = s(t) + j(t) \quad . \tag{89}$$

The intended transmission and jamming signal are assumed to have the general forms

$$s(t) = A_s(t) \cos \left[\omega_0 t + \phi_s(t)\right] \tag{90}$$

and

$$j(t) = A_j(t) \cos \left[\omega_1 t + \phi_j(t)\right] \quad . \tag{91}$$

We assume that the reference signal has the form,

$$\begin{aligned} X_1(t) = {} & C_1 A_s(t) \cos \left[\omega_0 t + \phi_s(t) + \theta_1\right] \\ & + C_2 A_j(t) \cos \left[\omega_1 t + \phi_j(t) + \theta_2\right], \end{aligned} \tag{92}$$

where θ_1 and θ_2 are constant phase angles, and C_1 and C_2 are real constants.

The quarter-wavelength delay introduces a 90-deg phase shift in both components of equation (92) if $\omega_0 \simeq \omega_1$. Thus,

$$\begin{aligned} X_2(t) = {} & C_1 A_s(t) \sin \left[\omega_0 t + \phi_s'(t) + \theta_1\right] \\ & + C_2 A_j(t) \sin \left[\omega_1 t + \phi_j'(t) + \theta_2\right]. \end{aligned} \tag{93}$$

In general, since $s(t)$ is unsynchronized with $j(t)$, we can make the approximation,

$$\frac{1}{\tau} \int_{t-\tau}^{t} s(t')j(t')dt' \simeq 0 \quad . \tag{94}$$

If $s(t)$ and $j(t)$ are regarded as zero-mean, ergodic processes and τ is sufficiently large, then the integral in equation (94) is an approximation of the expected value. In this case, the equation indicates that $s(t)$ and $j(t)$ are uncorrelated. With a similar

justification, we neglect all integrals involving the product of the jamming and intended transmission waveforms. Because of the bandpass filters, the modulation functions are slowly varying relative to $\omega_0 t$. We assume that $\omega_0\tau$, $\omega_1\tau >> 1$. Thus, equations (89) through (94) and simple trigonometry imply that

$$\int_{t-\tau}^{t} X_1(t')X_2(t')dt' << \int_{t-\tau}^{t} X_1^2(t')dt' . \tag{95}$$

Assuming that $W_1(t)$ and $W_2(t)$ are comparable in magnitude, equation (95) implies that we can neglect the final term in equation (88). Thus,

$$W_1(t) = \frac{K\int_{t-\tau}^{t} X_0(t')X_1(t')dt'}{1 + K\int_{t-\tau}^{t} X_1^2(t')dt'} . \tag{96}$$

For a sufficiently large value of K, we have the approximation,

$$W_1(t) \simeq \frac{\int_{t-\tau}^{t} X_0(t')X_1(t')dt'}{\int_{t-\tau}^{t} X_1^2(t')dt'} . \tag{97}$$

In an analogous manner, we obtain

$$W_2(t) \simeq \frac{\int_{t-\tau}^{t} X_0(t')X_2(t')}{\int_{t-\tau}^{t} X_2^2(t')dt'} . \tag{98}$$

The signal-to-jamming ratio at the reference input is defined to be

$$\rho_r = \frac{C_1^2\int_{t-\tau}^{t} s^2(t')dt'}{C_2^2\int_{t-\tau}^{t} j^2(t')dt} \simeq \frac{C_1^2\int_{t-\tau}^{t} A_s^2(t')dt'}{C_2^2\int_{t-\tau}^{t} A_j^2(t')dt'} . \tag{99}$$

It is assumed that τ is sufficiently large that ρ_r is nearly a constant. From this definition and the previous assumptions, we have

$$\int_{t-\tau}^{t} X_1^2(t')dt' = \frac{C_2^2\left(1 + \rho_r\right)}{2} \int_{t-\tau}^{t} A_j^2(t')dt' \quad , \tag{100}$$

and

$$\int_{t-\tau}^{t} X_0(t')X_1(t')dt' = \frac{C_2}{2C_1}\left(C_1\cos\theta_2 + C_2\rho_r\cos\theta_1\right)\int_{t-\tau}^{t} A_j^2(t')dt' \quad . \tag{101}$$

From equations (97), (100), and (101), we obtain

$$W_1(t) = \frac{C_1\cos\theta_2 + C_2\rho_r\cos\theta_1}{C_1C_2\left(1 + \rho_r\right)} \quad . \tag{102}$$

In an analogous manner, we derive

$$W_2(t) = \frac{C_1\sin\theta_2 + C_2\rho_r\sin\theta_1}{C_1C_2\left(1 + \rho_r\right)} \quad . \tag{103}$$

We now substitute into equation (84), and employ trigonometric identities. Defining the signal-to-jamming ratio at the primary input by

$$\rho_i = \frac{\int_{t-\tau}^{t} s^2(t')dt'}{\int_{t-\tau}^{t} j^2(t')dt'} = \frac{C_2^2\rho_r}{C_1^2} \quad , \tag{104}$$

we obtain the final result, assuming $\phi_j \simeq \phi_j'$ and $\phi_s \simeq \phi_s'$,

$$\left(1 + \rho_r\right)y(t) = s(t) + \rho_r j(t) - \sqrt{\frac{\rho_r}{\rho_i}}\,A_s\cos\left(\omega_0 t + \phi_s + \theta_1 - \theta_2\right)$$

$$-\sqrt{\rho_r\rho_i}\,A_j\cos\left(\omega_1 t + \phi_j - \theta_1 + \theta_2\right) . \tag{105}$$

If $\rho_r << \rho_i$, the second and third terms on the right-hand side can be neglected.[1] Treating ρ_i and ρ_r as constants, the signal-to-jamming ratio at the output of the sidelobe canceller is

$$\rho_0 \simeq \frac{1}{\rho_r \rho_i} \frac{\int_{t-\tau}^{t} s^2(t')dt'}{\int_{t-\tau}^{t} j^2(t')dt'} = \frac{1}{\rho_r}, \quad \rho_r << \rho_i \quad . \tag{106}$$

Thus, the jamming component of the primary signal has been nearly cancelled if $\rho_r << 1$. Within the accuracy of the approximations made, $y(t) \simeq s(t)$ if $\rho_r = 0$, that is, if there is no energy at the reference antenna from the intended transmission. In order for ρ_0 to exceed ρ_i, it is necessary and sufficient that $\rho_r \rho_i < 1$.

The fact that $\rho_0 = 1/\rho_r$ has been established for a somewhat different, sampled-data system in Widrow et al.[16] We conclude that the output signal distortion is small when the signal power at the reference antenna is relatively low.

If the jamming source is almost directly behind the source of the intended transmission, then $\rho_r \simeq \rho_i$ and $\theta_1 \simeq \theta_2$. Since equation (105) indicates that $y(t) \simeq 0$, the output signal is buried in the thermal noise. We conclude that the sidelobe canceller is ineffective in this case.

8. OPTICAL COMMUNICATION

Recent advances in optical fiber technology[17] have made optical communication systems both feasible and attractive in certain communication warfare environments. Because optical fibers do not emit a significant amount of electromagnetic energy, they are very effective in preventing the detection and interception of communications by an opponent. Tapping is more difficult than it is for an electrical cable. Since ambient electromagnetic energy does not interfere significantly with the propagation of optical waves in fibers, communication by means of optical fibers is nearly invulnerable to jamming. Other advantages of optical fibers are their light weight, resistance to fire, lack of "cross-talk" among fibers, and freedom from short circuits. Although it may not be necessary in many military communication systems, optical fibers can carry a much higher message density than metallic conductors of comparable dimensions. For military applications, the major disadvantage of optical fibers relative to ordinary electrical cables appears to be the difficulty of rapidly repairing damaged fibers.

---

[16] *B. Widrow et al, Adaptive Noise Cancelling: Principles and Applications, Proceedings of the IEEE, 63 (December 1975), 1692-1716.*

[17] *W. S. Boyle, Light-Wave Communications, Scientific American, 237 (August 1977), 41-48.*

LITERATURE CITED

(1) L. E. Follis and R. D. Rood, Jamming Calculations for FM Voice Communications, Electronic Warfare (November/December 1976), 33-40.

(2) N. M. Blachman, Noise and its Effects on Communication, McGraw-Hill (1966).

(3) R. E. Ziemer and W. H. Tranter, Systems, Modulation, and Noise, Houghton Mifflin (1976).

(4) H. Taub and D. L. Schilling, Principles of Communication Systems, McGraw-Hill (1971).

(5) C. Helstrom, Statistical Theory of Signal Detection, 2nd edition, Pergamon Press (1968).

(6) R. Pettit, Error Probability for NCFSK with Linear FM Jamming, IEEE Transactions on Aerospace and Electronic Systems, AES-8 (September 1972), 609-614.

(7) H. Feistel, Cryptography and Computer Privacy, Scientific American, 228 (May 1973), 15-23.

(8) D. J. Torrieri, Cryptographic Digital Communication, IEEE Transactions on Aerospace and Electronic Systems, AES-12 (January 1976), 2-11.

(9) H. L. Van Trees, Detection, Estimation, and Modulation Theory, III, Wiley (1971).

(10) R. C. Dixon, Spread Spectrum Systems, Wiley (1976).

(11) Spread Spectrum Communications, National Technical Information Service, AD-766-914 (1973).

(12) H. Urkowitz, Energy Detection of Unknown Deterministic Signals, Proceedings of the IEEE, 55 (April 1967), 523-531.

(13) A. Papoulis, Probability, Random Variables, and Stochastic Processes, McGraw-Hill (1965), 294, 341.

(14) W. F. Gabriel, Adaptive Arrays--An Introduction, Proceedings of the IEEE, 64 (February 1976), 239-272.

(15) B. Widrow, P. E. Mantey, L. J. Griffiths, and B. B. Goode, Adaptive Antenna Systems, Proceedings of the IEEE, 55 (December 1967), 2143-2159.

(16) B. Widrow et al, Adaptive Noise Cancelling: Principles and Applications, Proceedings of the IEEE, 63 (December 1975), 1692-1716.

(17) W. S. Boyle, Light-Wave Communications, Scientific American, 237 (August 1977), 41-48.

DISTRIBUTION

DEFENSE DOCUMENTATION CENTER
CAMERON STATION, BUILDING 5
ATTN DDC-TCA (12 COPIES)
ALEXANDRIA, VA 22314

COMMANDER
USA RSCH & STD GP (EUR)
BOX 65
ATTN LTC JAMES M. KENNEDY, JR.
CHIEF, PHYSICS & MATH BRANCH
FPO NEW YORK 09510

COMMANDER
US ARMY MATERIEL DEVELOPMENT
& READINESS COMMAND
ATTN DRXAM-TL, HQ TECH LIBRARY
ATTN DRCDE-DC/FIO, COL J. MIKULA
5001 EISENHOWER AVENUE
ALEXANDRIA, VA 22333

COMMANDER
USA MISSILE & MUNITIONS
CENTER & SCHOOL
ATTN ATSK-CTD-F
REDSTONE ARSENAL, AL 35809

DIRECTOR
US ARMY BALLISTIC RESEARCH LABORATORY
ATTN DRDAR-TSB-S (STINFO)
ABERDEEN PROVING GROUND, MD 21005

COMMANDER
US ARMY RESEARCH OFFICE
ATTN COL A. SIMKUS
P.O. BOX 12211
RESEARCH TRIANGLE PARK, NC 27709

COMMANDER
US ARMY AVIATION RESEARCH &
DEVELOPMENT COMMAND
ATTN MR. R. LEWIS,
ACTING TECHNICAL DIR
ST. LOUIS, MO 63166

COMMANDER
US ARMY TANK-AUTOMOTIVE RESEARCH
& DEVELOPMENT COMMAND
ATTN COL W. PALMER
TARAD LABS
WARREN, MI 48090

COMMANDER
US ARMY MISSILE RESEARCH
& DEVELOPMENT COMMAND
ATTN DR. J. KOBLER,
DIRECTOR TECHNOLOGY LAB
REDSTONE ARSENAL, AL 35809

COMMANDER/DIRECTOR
COMBAT SURVEILLANCE
& TARGET ACQUISITION LABORATORY
ATTN DELCS, COL W. EVANS
FT. MONMOUTH, NJ 07703

DIRECTOR
ELECTRONIC WARFARE LABORATORY
ATTN DELEW, MR. C. HARDIN
FT. MONMOUTH, NJ 07703

DIRECTOR
SIGNALS WARFARE LABORATORY
ATTN DELSW, MR. H. HOVEY
ARLINGTON HALL STATION
ARLINGTON, VA 22212

US ARMY COMMUNICATIONS RESEARCH
& DEVELOPMENT COMMAND
ATTN MG H. DICKINSON
FT. MONMOUTH, NJ 07703

COMMANDER
US ARMY INTELLIGENCE
& THREAT ANALYSIS DETACHMENT
ATTN ELECTRONIC WARFARE,
LTC J. V. COLE
ARLINGTON HALL STATION
ARLINGTON, VA 22212

COMMANDER
US ARMY FOREIGN SCIENCE
& TECHNOLOGY CENTER
ATTN DRXST-CE1, MR. EDWARD WEBSTER
ATTN DRXST-CE3, MAJ KENNETH KOPECKY
ATTN DRXST-CE2, MR. WILLIAM YOST
ATTN DRXST-CE, MR. A. RICCIARDELLI
220 SEVENTH STREET NE
CHARLOTTESVILLE, VA 22901

COMMANDER
MISSILE INTELLIGENCE AGENCY
ATTN DRDMI-Y, COL JACK WILSON
REDSTONE ARSENAL
HUNTSVILLE, AL 35809

DISTRIBUTION (Cont'd)

HARRY DIAMOND LABORATORIES
ATTN COMMANDER/
FLYER, I.N./LANDIS, P.E./
SOMMER, H./OSWALD, R. B.
ATTN CARTER, W.W., DR., TECHNICAL DIRECTOR
ATTN WISEMAN, ROBERT S., DR., DRDEL-CT
ATTN HOYT, L., COL, DRDEL-DE
ATTN MURRAY, G., COL, DRDEL-AP-CCM (6 COPIES)
ATTN MARCUS, S. M., 003
ATTN KIMMEL, S., PAO
ATTN CHIEF, 0021
ATTN CHIEF, 0022
ATTN CHIEF, LAB 100
ATTN CHIEF, LAB 200
ATTN CHIEF, LAB 300
ATTN CHIEF, LAB 400
ATTN CHIEF, LAB 500
ATTN CHIEF, LAB 600
ATTN CHIEF, DIV 700
ATTN CHIEF, DIV 800
ATTN CHIEF, LAB 900
ATTN CHIEF, LAB 1000
ATTN RECORD COPY, BR 041
ATTN HDL LIBRARY (5 COPIES)
ATTN CHAIRMAN, EDITORIAL COMMITTEE
ATTN CHIEF, 047
ATTN TECH REPORTS, 013
ATTN PATENT LAW BRANCH, 071
ATTN GIDEP OFFICE, 741
ATTN LANHAM, C., 0021
ATTN TORRIERI, D. J., (25 COPIES)